(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 June 2006 (08.06.2006)

PCT

(10) International Publication Number
WO 2006/059190 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IB2005/003281

(22) International Filing Date:
8 November 2005 (08.11.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/IB2004/03899
8 November 2004 (08.11.2004) IL

(71) Applicant *(for all designated States except US)*: **IDESIA LTD.** [IL/IL]; 7, Halamish St., 38900 Caesarea (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LANGE, Daniel, H.** [IL/IL]; Yarden 10, P.O. Box 939, 25147 Kfar Vradim (IL).

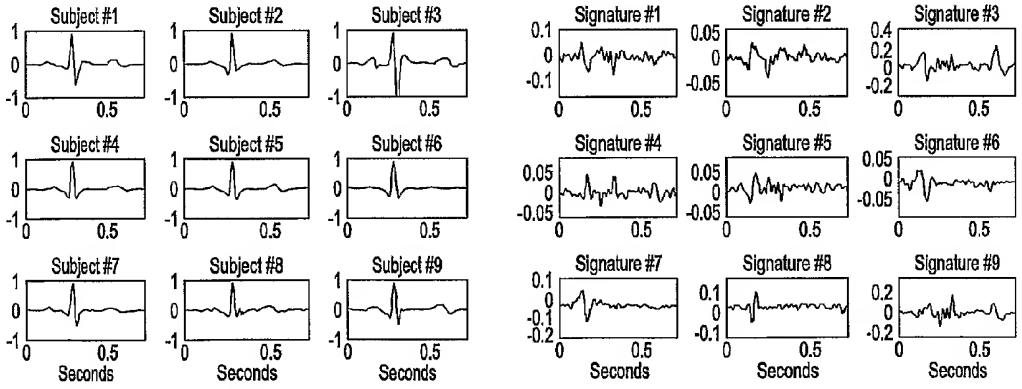
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** METHOD AND APPARATUS FOR ELECTRO-BIOMETRIC IDENTITY RECOGNITION



ORIGINAL ELECTROCARDIOGRAPHIC SIGNALS (LEFT)
COMMON-ELIMINATED DERIVED SIGNATURES (RIGHT)

(57) **Abstract:** A method and apparatus for electro-biometric identity recognition or verification that produces and stores a first biometric signature that identifies a specific individual by forming the difference between a representation of the heartbeat pattern of the specific individual and a stored representation of common features of the heartbeat patterns of a plurality of individuals; after the producing step, the method and apparatus obtains a representation of the heartbeat pattern of a selected individual and produces a second biometric signature by forming the difference between the heartbeat pattern of the selected individual and the stored representation of common features of the heartbeat patterns of the plurality of individuals; it then compares the second biometric signature with the first biometric signature to determine whether the selected individual is the specific individual. The apparatus and method may be employed as a stand-alone unit or as part of another device pursuant to the many applications described herein.

WO 2006/059190 A2

DESCRIPTION

Method and Apparatus for Electro-Biometric Identity Recognition

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority to PCT Application No. PCT/IB04/03899, filed on November 8, 2004, which is a continuation-in-part of International Patent Application No. PCT/US2003/23016, filed on July 24, 2003, which claims benefit of U.S. provisional application 60/398,832, filed on July 29, 2002, the entire disclosures of which are incorporated herein by reference.

BACKGROUND

Identity recognition plays an important role in numerous facets of life, including automatic banking services, e-commerce, e-banking, e-investing, e-data protection, remote access to resources, e-transactions, work security, anti-theft devices, criminologic identification, secure entry, and entry registration in the workplace.

Often computerized systems use passwords and personal identification numbers (PIN) for user recognition. But to maintain security, passwords have to be changed on a regular basis, imposing a substantial burden on the users. Likewise, signature verification methods suffer from other shortcomings, including forgery and enrollment fraud. See for example, U.S. Patent No. 5,892,824 issued to Beatson et al.

As a result, identity recognition systems that use measures of an individual's biological phenomena — biometrics — have grown in recent years. Utilized alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures, biometrics are

expected to pervade nearly all aspects of the economy and our daily lives.

Several advanced technologies have been developed for biometric identification, including fingerprint recognition, retina and iris recognition, face recognition, and voice recognition. For example, Shockley et al., U.S. Pat. No. 5,534,855, generally describes using biometric data, such as fingerprints, to authorize computer access for individuals. Scheidt et al., U.S. Patent No. 6,490,680, describes identity authentication using biometric data. Dulude et al., U.S. Patent No. 6,310,966, describes the use of fingerprints, hand geometry, iris and retina scans, and speech patterns as part of a biometric authentication certificate. Murakami et al., U.S. Patent No. 6,483,929, generally describes "physiological and histological markers," including infra-red radiation, for biometric authentication. However, these types of technologies have penetrated only limited markets due to complicated and unfriendly acquisition modalities, sensitivity to environmental parameters (such as lighting conditions and background noise), and high cost. In addition, due to complicated acquisition procedures, the foregoing technologies usually require operator attendance.

Fingerprint recognition is well-established and the most mature technology of the group. But it has several drawbacks: a fingerprint recognition system cannot verify physical presence of the fingerprint owner and therefore is prone to deception, limiting its suitability for on-line applications; the optical sensor is a costly and fragile device generally unsuitable for consumer markets; and the system suffers from negative connotations related to criminology.

Retina scanning technologies are characterized by high performance. However, they require high-precision optical sensors, and are not user friendly because they require manipulation of head posture and operate on a very sensitive organ — the human eye. The optical sensor is also costly and fragile.

Iris and face recognition systems are user-friendly technologies since they record an image from afar and are not intrusive. However, they require digital photographic equipment and are sensitive to lighting conditions, pupil size variations and facial expressions. In addition, iris recognition performance is degraded by the use of dark glasses and contact lens, and face recognition may be deceived by impersonation.

Voice recognition is the most user-friendly technology of the group; however, it requires a low-noise setting and is highly sensitive to intrinsically variable speech parameters, including intonation. Moreover, existing conventional recording technologies may be used to deceive speech-based recognition systems.

Thus, a need exists for reliable, robust, hard to deceive (on-line and off-line), low cost, user friendly identity recognition technologies that may be used in stand-alone applications or integrated with existing security systems.

Over the years, electrocardiogram ("ECG") measurements have been used for many different purposes. ECG signals are electric signals generated by the heart and can be picked up using conventional surface electrodes, usually mounted on the subject's chest. ECG signals are made up of several components representative of different functional stages during each heart beat and projected according to the electric orientation of the generating tissues.

Individuals present different, subject-specific detail in their electro-cardiologic signals due to normal variations in the heart tissue structure, heart orientation, and electrical tissue orientation, all of which affect the electro-cardiologic signals measured from the limbs. Numerous types of systems make use of these subject-specific variations.

For example, Blazey et al., U.S. Patent No. 6,293,904, describes the use of ECG signals to evaluate or profile an individual's physiological and cognitive state. As to identification, a 2001 conference paper at the 23rd Annual International IEEE Conference on Engineering in Medicine and Biology Society (in Istanbul, Turkey) by Kyoso et al., entitled "Development of an ECG Identification System," compares a patient's ECG with previously registered ECG feature parameters for purposes of identification. Wiederhold, U.S. Application No. 2003013509, suggests using directly or remotely acquired ECG signals to identify a subject, "explores" feature extraction for identifying individuals, and provides a "preliminary analysis" of such methods.

But an ECG signal is comprised of ECG components having features that may be common to a group. None of these references describe a system or method that eliminates common features of ECG components to create a signature for subject identification. Thus, there still exists a need for systems and methods with these attributes to identify an individual.

The inclusion of the foregoing references in this Background is not an admission that they are prior art or analogous art with respect to the inventions disclosed herein. All references in this Background section are,

however, hereby incorporated by reference as though fully set out herein.

SUMMARY

Applicant provides solutions to the foregoing problems of biometric identification with various apparatuses and methods having several aspects.

In a first aspect, applicant solves each of the foregoing problems of biometric identification through the use of the following method and variations thereof:

producing and storing a first biometric signature that identifies a specific individual by forming the difference between a representation of the heartbeat pattern of the specific individual and a stored representation of common features of heartbeat patterns of a plurality of individuals;

after the producing step, obtaining a representation of the heartbeat pattern of a selected individual and producing a second biometric signature by forming the difference between the heartbeat pattern of the selected individual and the stored representation of the common features of the heartbeat patterns of the plurality of individuals; and

comparing the second biometric signature with the first biometric signature to determine whether the selected individual is the specific individual.

A system, according to this aspect, comprises an ECG signal acquisition module, an ECG signal processing module that comprises an ECG signature generator, and an output module.

Thus, according to this first aspect, the systems and methods disclosed herein transform bio-electric signals into unique electro-biometric signatures. The uniqueness of the

electro-cardiologic signatures makes the system very difficult to deceive, and the method's inherent robustness makes it ideal for local as well as for remote and on-line applications. In addition, a biometric-signature-based system is characterized by high recognition performance and supports both open and closed search modes.

In one preferred method according to the first aspect, the stored representation of common features of one or more ECG components is obtained by measuring and storing such representations for a plurality of individuals and then averaging all of the stored representations. Alternately, the common features may be obtained through techniques such as principal component analysis, fuzzy clustering analysis, wavelet decomposition, and the like.

Since electro-cardiologic methods according to this first aspect are robust, they have another important advantage: they permit a simple and straightforward acquisition technology that can be implemented as a low-cost, user friendly acquisition apparatus and also eliminate the need for a skilled operator.

According to a variation on these systems and methods, the common features of one or more of a subject's ECG components may be removed using an analytical model of common features of one or more ECG components, instead of, or in addition to, use of an empirical model. Likewise, the common features may be removed by first classifying the stored representations into subgroups, identifying the common features in at least one subgroup, classifying a subject signal according to subgroup, creating a subject signature by removing the common features of one or more of the subgroup's ECG components from the subject signal, and identifying the subject by calculating the subject signature correlations relative to that subgroup's signatures.

Common features may be determined by averaging synchronized electrocardiograms from a group of individuals and then subtracted from the subject's electrocardiogram to determine the subject's signature. But this method assumes that common features are constant across a group of individuals. In reality, certain common features are present to a greater or lesser degree in any given individual. Therefore, it is better to approximate common features so they make the best fit with a given subject's electrocardiogram before removing them to obtain the subject's signature. This technique provides for a more accurate determination of the subject's signature.

According to this method, a group of electrocardiograms may be broken down (decomposed) into a set of characteristic waveforms. The characteristic waveforms that represent common features of the group are then weighted to best approximate the extent of common features present in the subject's electrocardiogram. The approximation is then subtracted from the subject's electrocardiogram. What remains includes the subject's electrocardiogram signature.

Multiple templates may also be kept for each subject, such as by storing multiple signatures produced by an individual at different pulse rates. In this embodiment, the subject signature may then be correlated with the appropriate template, such as the one for the appropriate pulse rate. Thus, in a variation, the systems and methods disclosed herein may use multiple signature templates to identify an individual over a range of circumstances and reactions. Alternatively, or in addition, according to the first aspect, the subject signal and the enrolled signals may also be normalized based on pulse rate.

According to a second aspect disclosed herein, a process for identification may set a dynamic threshold.

This dynamic threshold may be based on a desired level of confidence in the identification, such as one determined by a confidence score.

According to a third aspect disclosed herein, the systems and methods disclosed herein may employ a "Q-factor" to determine whether to reduce signal contamination due to noise. Likewise, the Q-factor or other quality of signal measurement may be used to determine the length of the subject sample required to identify a subject with a desired level of confidence. It may also be used to enroll a sample with the desired level of confidence so that the sample may be suitable for the future comparison.

In an alternate embodiment to the "Q-factor" calculation, the systems and methods disclosed herein may calculate standard deviations in the subject signature and/or enrolled signatures due to noise, and from those calculations determine whether signal quality is appropriate for identification.

Likewise, the systems and methods disclosed herein may determine the signal quality by measuring the impedance of the contact or probe. Signal quality measurements according to this aspect may also be used to inform the subject to adjust his or her contact with or position relative to the sensor or probe.

According to a fourth aspect, the subject and database signatures may be encrypted as a safety precaution against unauthorized access to and use of the signatures.

According to a fifth aspect, the ECG signal may be acquired with electrodes placed in contact with certain body sites that yield a consistent signal. For certain body locations even a slight change of electrode placement may cause drastic changes in the received signal morphology, and may even cause distinct signal components to appear or

disappear. Thus, according to this aspect, the methods and systems disclosed herein may use electrode placement sites that produce subject-specific, consistent signals, that are robust notwithstanding changes of electrode placement within the sites. These sites include the arms and legs (including fingers and toes). The robustness of electrode placement within these sites stems from a constant electro-cardiologic signal projection which does not change as long as the electrodes remain close to a limb extremity.

According to this same fifth aspect, certain sensing probes, known as ultra-high impedance sensing probes, may also be used to acquire a signal, including a signal from a single body point such as a fingertip. Alternately, or in addition, these ultra-high impedance probes may remotely sense the electro-cardiologic signal and thereby eliminate the difficulty of electrode placement while maintaining signal consistency.

According to a sixth aspect, the systems and methods disclosed herein may comprise elements and steps that protect against enrollment fraud and reduce the ability of a database enrollee to misrepresent his or her identity.

According to a seventh aspect, the systems and methods disclosed herein may identify a subject by comparing his or her match scores with the match scores of database enrollees.

According to an eighth aspect, the systems and methods disclosed herein may use weighted correlation techniques, ascribing different weights to different electro-cardiologic signal components for the purpose of producing a signature. Alternatively, or in addition, signatures may be normalized using a variety of metrics including root-mean-square computations or L1 metrics.

Some biometric technologies employ challenge-response protocols to ensure that the user data that they receive is live. In that way, they can reduce the risk that the system can be spoofed by the playback of biometric data. But, to date, the challenge-response mechanisms for biometric systems have required active participation by the user. And active user participation complicates and extends the user verification process. For example, speech recognition systems typically require the user to repeat a randomly selected word or sentence. Therefore, according to another aspect, a biometric ID system may reduce the risk of spoofing by beneficially employing a biological-challenge-response mechanism that does not require a conscious response from the user.

The systems and methods according to each of the foregoing aspects preferably perform their tasks automatically for the purpose of identity recognition. Further, these systems and methods can be incorporated into a wide range of devices and systems. A few non-limiting examples are as follows: a smart card; a passport; a driver's license apparatus; a Bio-logon identification apparatus; a personal digital assistant ("PDA"); a cellular-embedded identification apparatus; an anti-theft apparatus; an ECG monitoring apparatus; an e-banking apparatus; an e-transaction apparatus; a pet identification apparatus; a physical access apparatus; a logical access apparatus; and an apparatus combining ECG and fingerprint monitoring, blood pressure monitoring and/or any other form of biometric device.

Further, the systems and methods disclosed herein can be used to identify a person's age, such as by comparing the width of a subject's QRS complex, or more generally the

subject's QRS-related signature component, with those of an enrolled group or analytical ECG model.

In another application, the systems and methods herein may be used to identify persons on medication, such as by enrolling and calculating, or analytically deriving, a series of drug-related signature templates. This method may also be used to identify or catch subjects who would attempt to fool the system by using medication to alter their ECG signal.

Other applications include using the systems and method disclosed herein for building and room access control, surveillance system access, wireless device access, control and user verification, mobile phone activation, computer access control (including via laptop, PC, mouse, and/or keyboard), data access (such as document control), passenger identification on public transportation, elevator access control, firearm locking, vehicle control systems (including via ignition start and door locks), smart card access control and smart card credit authorization, access to online-line material (including copyright-protected works), electronic ticketing, access and control of nuclear material, robot control, aircraft access and control (passenger identity, flight control, access of maintenance workers), vending machine access and control, laundromat washer/dryer access and control, locker access, childproof locks, television and/or video access control, decryption keys access and use, moneyless slot machines, slot machine maintenance access, game console access (including on-line transaction capability), computer network security (including network access and control), point-of-sale buyer identification, on-line transactions (including customer identification and account access), cash payment service or wire transfer identification, building maintenance access

and control, and implanted medical device programming control. Other applications will be apparent to those skilled in the art and within the scope of this disclosure.

For any application, an apparatus according to any or all of the foregoing aspects can operate continuously or on demand. The apparatus can be constructed to obtain the representation of the heartbeat pattern of a selected individual by having one or more electrodes in contact with individual or sensors remote from the individual. When the apparatus is provided in a smart card, the card can be enabled for a limited period of time after successful recognition and disabled thereafter until the next successful recognition is performed. The apparatus can be constructed to operate with encryption keys or digital signatures.

As to the methods disclosed herein, the steps of the foregoing methods may be performed sequentially or in some other order. The systems and methods disclosed herein may be used on human or other animal subjects.

Each of these aspects may be used in permutation and combination with one another. Further embodiments as well as modifications, variations and enhancements are also described herein.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a simplified block diagram of a system for use with the aspects disclosed herein composed of a signal acquisition module, a signal processing module, and an output module.

FIG. 2 is a block diagram of an embodiment of the signal acquisition module of the system of **FIG. 1.**

FIG. 3 is a block diagram of an embodiment of the signal processing module of the system of **FIG. 1.**

FIG. 4 shows the first six most influential PCs extracted from a pool of one-hundred subjects, and the contribution of the first ten PCs to the representation of data variance.

FIG. 5 shows the original electrocardiographic signals and their respective signatures constructed by eliminating the optimal combination of the three most influential PCs and their latency shifted versions.

FIG. 6 is a diagram showing a grand-average electro-cardiologic signal waveform calculated from a database of 20 subjects.

FIG. 7 shows a group of electro-cardiologic signal waveforms of ten of the subjects participating in the database and contributing to the average waveform of **FIG. 4.**

FIG. 8 shows a group of electro-biometric signature waveforms, or templates, derived from the signal waveforms of **FIG. 7.**

FIG. 9 shows a scatter plot and distribution histograms of the sign-maintained squared correlation values of the 20 subjects who contributed to the grand average waveform of **FIG. 4.**

FIG. 10 shows a table of z-scores based on the desired degree of confidence in the identification cut-off.

FIG. 11a shows a distribution of correlation.

FIG. 11b shows a distribution of Z-transformed correlations.

FIG. 12 shows identification performance curves (static).

FIG. 13 shows identification performance curves (dynamic).

FIG. 14 shows signal quality as a function of NSR.

FIG. 15 shows match score distribution as a function of signal quality for 5 second segments.

FIG. 16 shows match score distribution as a function of signal quality for 20 second segments.

FIG. 17 shows match score as a function of recording duration (for Q=0.8).

FIG. 18 shows match score as a function of recording duration (for Q=0.5).

FIG. 19 shows a functional component diagram of a preferred system.

FIG. 20 shows a functional component diagram of a preferred signal processor.

DETAILED DESCRIPTION

Definitions:

Unless otherwise indicated, the meaning of the terms "identify," "identifying" and "identification" include the concepts of "verify identity," "verifying identity," and "verification of identity," respectively.

"Closed search" means a search in which a single stored signature is examined to verify the identity of an individual.

"Open search" means a search in which a plurality of stored signatures are searched to identify a subject.

First Aspect:

According to the first aspect, a bio-electric signal is acquired, processed and analyzed to identify the identity of an individual. A preferred embodiment of a system and a method according to this first aspect is illustrated, by way of example, in **FIG. 1**. **FIG. 1** shows a system called an **E**lectro-**Bio**metric **ID**entification (E-BioID) system. In this preferred embodiment, the stored representation of the common features of the one or more ECG components of the

plurality of individuals is the average of those individuals' one or more ECG components. However, other embodiments can utilize stored representations of different types of common features, such as those attainable by, for example, principal component analysis, fuzzy clustering analysis, or wavelet decomposition, or provided by an analytical model.

In the preferred embodiment, the basic elements of the E-BioID system include a signal acquisition module 12, a signal processing module 14, and an output module 16, implemented in a single housing. In another preferred embodiment, the system may provide for remote analysis of locally acquired electro-biometric signals. Each of the components shown in **FIG. 1** can be readily implemented by those skilled in the art, based on principles and techniques already well known in the art in combination with the present disclosure.

FIG. 2 shows a preferred construction of the signal acquisition module 12 in an E-BioID system. The data acquisition module preferably includes one or more sensors 22, pre-amplifiers 24, band-pass filters 26 and an analog-to-digital (A/D) converter 28. Each of these components can be readily implemented by those skilled in the art, based on principles and techniques already well known in the art in combination with the present disclosure.

Sensors 22 can be of any type capable of detecting the heartbeat pattern. For example, they can be metal plate sensors that are an "add-on" to a standard computer keyboard. According to another aspect, a single sensor may, by itself, acquire the signal from a single point of contact, such as by contacting a finger; alternately, the sensor may not need to touch the subject at all.

FIG. 3 shows preferred elements of signal processing module 14 in the E-BioID system. The signal processing module preferably includes a Digital Signal Processor (DSP) 32, a Dual Port Ram (DPR) 34, an Electrically Erasable Programmable Read Only Memory (E^2PROM) 36 and an I/O port 38. Each of these components can be readily implemented by those skilled in the art, based on principles and techniques already well known in the art in combination with the present disclosure. Signal processing module 14 is connected to signal acquisition module 12 and output module 16 via port 38.

In an alternative embodiment, the signal processing module may be implemented, with suitable programming, on a personal computer, which is a flexible computation platform, allowing straight-forward integration of the system into existing computing facilities in a home, office, or institute/enterprise environments.

Output module 16 preferably consists of a dedicated display unit such as an LCD or CRT monitor, and may include a relay for activation of an external electrical apparatus such as a locking mechanism. Alternatively, the output module may include a communication line for relaying the recognition result to a remote site for further action.

SIGNAL ACQUISITION, PROCESSING AND ANALYSIS

Bioelectric signals, or heartbeat signals, are acquired in a simple manner, where the subject is instructed to touch at least one sensor 22 for a few seconds. The one or more sensors, which may be metal plates, conduct the bioelectric signals to the amplifiers 24, which amplify the bioelectric signals to the desired voltage range. In a preferred embodiment, the voltage range is zero to five volts.

The amplified signals pass through filters 26 to remove contributions outside a preferable frequency range of 4Hz – 40Hz. Alternatively, a wider range of 0.1Hz – 100Hz may be used in conjunction with a notch filter to reject mains frequency interference (50/60Hz). Digitization of the signal is preferably performed with a 12-bit A/D converter 28, at a sampling frequency of preferably about 250Hz.

In module 14, the signals are normalized by the 'R' peak magnitude, to account for signal magnitude variations which mostly relate to exogenic electrical properties. The normalized data is transformed into an electro-biometric signature which is compared to pre-stored electro-biometric signature templates. The result of the comparison is quantified, optionally assigned a confidence value, and then transmitted to output module 16, which provides recognition feedback to the user of the E-BioID system and may also activate external apparatuses such as a lock or siren, virtual apparatuses like network login confirmation, or a communication link.

Alternately, or in addition, the signal may be normalized for pulse rate. This is useful because electro-cardiologic signals are affected by changes in pulse rate, which is a well-known electro-cardiologic modifier. Pulse rate changes may cause latency, amplitude and morphological changes of the 'P' and 'T' components relative to the 'QRS' component of the electro-cardiologic signal (these components appear in **FIG. 7**). However, pulse rate changes may be automatically compensated for by retrospective, pulse rate-driven adjustment of the signal complex. Moreover, an adaptive operation mode of the system can track and compensate for pulse rate induced changes. This can be done by compressing or expanding the time scale of one cycle of the heartbeat waveform. More sophisticated formulations

describing the relations between waveform characteristics (*e.g.* S-T, P-Q segment durations) and pulse rate may be used. Thus, a method according to this variation may be based on electro-cardiologic signal discrimination, wherein analysis is carried out synchronously with the heart beat, eliminating features common to the general population and thus enhancing subject-specific features that constitute an electro-biometric, or biometric, signature, normally undetectable in raw electro-cardiologic signals.

In another embodiment, the E-BioID system is implemented as a fully integrated compact device, where many of the functional elements are implemented on an ASIC based system.

In another embodiment, the apparatus can be incorporated into a watch worn on the wrist, where the signal is measured between the wrist of the hand on which the watch is worn and the other hand of the wearer. The back side of the watch may be made of a conductive medium (*e.g.* a metal plate) in contact with the back of the wrist, and the face of the watch can be provided with another metal contact that needs to be touched with a finger of the other hand. The watch may transmit a signal indicating confirmation of the identity of its wearer, and/or activating a physically or logically locked device such as a door, a computer, a safe, etc. The watch may also transmit personal information about its wearer. In the same manner, the apparatus can be incorporated into a belt, or any other apparel item comprising a conductive medium. The belt or other apparel item may then transmit a signal indicating confirmation of the identity of its wearer, and/or activating a physically or logically locked device and/or transmitting personal information about its wearer.

PRINCIPLE OF OPERATION

Biometric recognition requires comparing a newly acquired biometric signature against signature templates in a registered or enrolled biometric signature template database. This calls for two phases of system operation: Enrollment and Recognition.

ENROLLMENT PHASE

In a preferred embodiment, each new subject is instructed to touch a first sensor with a finger of the left hand, while simultaneously touching another sensor with a finger of the right. In alternative embodiments, the subject may touch the sensors, typically made of metal, with other parts of the body, preferably the hands or legs. In another embodiment, the subject may touch a single sensor with a single body point. Alternately, the subject need not touch a sensor at all. The system monitors the subject's pulse rate and initiates a recording, preferably lasting for at least 20 seconds. Shorter intervals may be used depending on the required level of accuracy. Once the recording is complete, the system may perform a self-test to verify signature consistency by comparison of at least two biometric signatures derived from two parts of the registered segment. The two parts may be two halves, or two larger, overlapping, segments. The two parts may be used to derive two biometric signatures. If the self-test result is successful, enrollment of that subject is complete, and if unsuccessful the procedure is repeated. The successful recording is used for construction of an electro-cardiologic signal or a series of electro-cardiologic signals, which are added to an electro-cardiologic signal database.

The electro-cardiologic signals are then transformed into a set of electro-biometric signature templates by

eliminating features that are common to all or a subset of the subjects participating in the dataset, thereby enhancing subject-specific discriminating features.

In a preferred embodiment, the system creates a grand-average electro-cardiologic template, which is calculated by synchronous averaging of normalized electro-cardiologic signals from the entire pool of subjects. The grand-average represents the above-mentioned common features, and thus subtraction of the grand-average from each one of the electro-cardiologic signals yields a set of distinct, subject-specific electro-biometric template signatures. In an alternative embodiment, other means for elimination of the common features may be used, such as a principal component analysis, fuzzy clustering analysis or wavelet decomposition.

In a more preferred embodiment, a group of electrocardiograms may be broken down (decomposed) into set of characteristic waveforms. According to this preferred embodiment, noise is removed from the electrocardiograms of a group of individuals. The system may use Principal Component Analysis (PCA) to decompose the group's electrocardiograms into a set of orthogonal (non-correlated) components. These non-correlated components, taken together, represent the entire energy of the signals—that is 100% of the signal variance.

The first principal components—those associated with largest eigen values of the PCA representation. Usually the first three to five components and, in any event, less than the first ten components of the group's electrocardiograms typically represent approximately 90% of the electrocardiogram's energy or variance and contain the common features. Remarkably, these first components represent common features that are present and stable across

the human population at large. As a result, these first principal components can be used to identify the signature of any human subject and need not be recalculated for each subject. The remaining smaller components (which typically can be 10% of the total waveform energy) represent noise and some individual information of the group.

The characteristic waveforms that represent common features of the group are then subtracted from the subject's electrocardiogram. What remains includes the subject's electrocardiogram signature plus some remaining noise.

Characteristic waveforms may be created in different ways, and depend on the desired "distance" or "overlap" between each waveform. For example, the correlation function may preferably be used to determine the desired distance between waveforms, although other methods also work.

Remarkably, if an electrocardiogram is taken from an individual who has not participated in the enrollment data set, it is possible to determine his or her electrocardiogram signature usually with reference to just the first three to four PCA components of the enrolled data set and time shifted versions of them.

Determining the Signature

All subjects' electrocardiograms contain each of the first principal components to greater or lesser degrees. According to this preferred embodiment, a subject's electrocardiogram may be approximated using the principal components from the sample set according to the following equation.

$$\sum_{i=1}^{p} C_i PC_i = ECG_{individual}$$

In this equation, C_i is a reconstruction coefficient, p is the model order and PC is the principal component. The goal is to find the coefficients that weight the database principal components for the best approximation of the subject's electrocardiogram. In other words, the goal is to minimize the error between an approximation of the subject signal constructed by the weighting the database's principal components and the original subject signature.

This may be done by a variety of methods. One method is to determine reconstruction coefficients using a least squares approximation to minimize the norm of the reconstruction error. This is shown below:

$$\| \mathrm{ECG}_{ind} - \sum C_i PC_i \| \quad \mathrm{OR} \quad \mathrm{Error} = \sum_{n=1}^{N} \left(\mathrm{ECG}_n - \sum C_i \bullet PC_i \right)^2$$

Once the optimal coefficients are determined, they may be used to sum the database's first principal components (such as the top 3 or 4) according to the following equation:

$$\sum_{i=1}^{3 \text{ or } 4} C_i \bullet PC_i = \mathrm{Sum}$$

This sum is then subtracted from the subject signal. What remains is the subject signature and perhaps some noise.

Further, since noise, by definition, is uncorrelated, it is usually described by the last principal components — those that are associated with the smallest eigen values. As a result, noise may be optionally removed from the subject signal by weighting these last principal components to make the optimal fit with the subject signature and then removing them from the subject signal. Noise may also be removed by other methods.

Accounting for Latency Variation

Some of the variation in an electrocardiogram component database is due to latency changes, namely time variance in

enrolled data signatures. As a result, the foregoing method may be enhanced by time shifting the principal components, preferably both to the left and to the right. For example, if three principal components are used to approximate common electrocardiogram features, then six more components could be added to account for latency variation—two for each component, shifted left and shifted right.

In this example, the three principal components and the six time shifted components would be used to calculate the construction coefficients. And once the best construction coefficients are determined, the common feature components are constructed and subtracted from the original subject electrocardiogram signature to yield the individual signature:

$$\text{Signature} = \text{ECG}_n - \sum_{i=1}^{P} C_i \bullet \text{PC}_i$$

FIG. 4 shows the first six most influential PCs extracted from a pool of one-hundred subjects, and the contribution of the first ten PCs to the representation of data variance. **FIG. 5** shows the original electrocardiographic signals and their respective signatures constructed by eliminating the optimal combination of the three most influential PCs and their latency shifted versions.

Although PCA is a robust algorithm that provides a progressive, influential representation of components with clear distinctions in magnitude between the main signal, secondary variations and noise, at least two alternate techniques may be used to decompose the group's electrocardiograms. In a first alternate embodiment, independent component analysis (ICA) may be used to decompose compound signals into independent components (as opposed to the orthogonal components of PCA). These

independent components may then be used for modeling and reconstruction of electrocardiograms in a manner similar to PCA.

In a second alternate embodiment, wavelet decomposition (WD) may be used to decompose compound signals into a set of time-scaled waveforms called wavelets. WD is based on a transient wavelet waveforms, as opposed to Fourier decomposition (which is based on continuous sine and cosine decomposition). As a result, WD has an advantage over Fourier analysis in that wavelets are more efficient descriptors of transient signal components such as electrocardiograms.

Alternately, or in addition, common features may be removed by using an analytical model for common features of one or more ECG components rather than by using an empirical model calculated from the enrolled data.

In another preferred embodiment, the database is divided into several subsets in a way that enhances intra-subset similarity and inter-subset disparity. The embodiment then calculates a distinct grand-average or other common feature determination for one or more of the subsets. This database partition itself may be performed using standard pattern classification schemes such as linear classifiers, Bayesian classifiers, fuzzy classifiers, or neural networks. In case of a large database, it is useful to partition the database into subsets in order to simplify and shorten the search process as well as to ensure the validity of the grand-average as an appropriate representative of similarity among the electro-cardiologic signals. The subject signature may then be created by removing common features found in the appropriate subgroup.

FIG. 6 shows an example of a grand-average, constructed from a pool of 20 subjects participating in the database.

FIG. 7 shows 10 examples of electro-cardiologic signals, and **FIG. 8** shows the electro-biometric template signatures derived from the above electro-cardiologic signals by elimination of features common to all the subjects included in the database. Specifically, each signature of **FIG. 8** is obtained by subtracting the waveform of **FIG. 6** from the corresponding signal of **FIG. 7**. It will be observed that while the original electro-cardiologic signals are highly similar, the derived electro-biometric signatures are markedly different. These differences have been found to reflect inherently unique electro-cardiologic disparity which underlies the recognition capabilities of the E-BioID system.

RECOGNITION PHASE

In the recognition phase, the subject interacts with the system in a similar manner to that of the enrollment phase, however a shorter recording time on the order of a few seconds is sufficient.

In a preferred embodiment, the system executes a verification procedure (closed search): the system processes the acquired signals, forms an electro-biometric subject signature by removing common features found in the entire database, found in a partitioned subgroup of the database or provided by analytical ECG model, adjusts the signature according to the pulse rate, and compares the adjusted electro-biometric signature with the subject's enrolled electro-biometric signature template.

In another preferred embodiment, the system executes an identification procedure (open search): the system repeats the comparison process for the entire database or a partitioned sub-group of the database, thereby providing identification of the matching identity.

THE COMPARISON PROCESS

In a preferred embodiment, the comparison is performed by calculation of a correlation coefficient, ρ, between an electro-biometric signature σ_j and an electro-biometric signature template Φ_i, as follows:

$$\rho = \frac{COV[\sigma_j, \Phi_i]}{\sqrt{VAR[\sigma_j] \cdot VAR[\Phi_i]}} .$$

The correlation coefficient is squared, maintaining its original sign: $\eta = sign(\rho) * |\rho|^2$. In an alternative embodiment, the comparison may be based on other similarity measures, such as RMS error between the electro-biometric signatures.

The comparison may yield one or several correlation coefficients, depending on the mode of operation: closed search; or open search. In a closed search mode, the sign-maintained squared correlation coefficient (η) is used for making the recognition decision: a value greater than a preset threshold is regarded as a positive identification, or a match; borderline, near-threshold values may indicate a need for extended or repeated recording. In an open search mode, the largest sign-maintained squared correlation coefficient among all sign-maintained squared correlation coefficients yields the most likely subject identification, provided that the highest coefficient is above a selected threshold.

The preset threshold is derived from the required confidence level; higher desired confidence levels require higher thresholds. In one embodiment, sign-maintained squared correlation values larger than 0.8 are characteristic of a match and values lower than 0.7 are characteristic of a mismatch. Thus, sign-maintained squared correlation values higher than 0.8 may be considered as true matches and values lower than 0.7 as mismatches.

The upper diagrams of **FIG. 9** shows a scatter plot of sign-maintained squared correlation values, marking the 0.8 threshold with a dashed line. A clear separation between matches (circles) and mismatches (stars) is evident. The histograms in the other two diagrams provide a different view of the powerful recognition capabilities of the E-BioID system, where it can be seen that the mismatches are concentrated around the zero value (no correlation) while matches are densely distributed near 1.0 (absolute correlation).

In alternative embodiments, more sophisticated decision schemes may be used such as multi-parameter schemes (e.g. fuzzy logic schemes), which use more than one distance measure; for example, multiple correlation values can be derived from segmented data analysis.

In a preferred embodiment, the system improves its performance with time by adding electro-cardiologic signals to the subject's database file when changes in the signals are encountered. In subsequent recognitions, the system processes the newly acquired signals, calculates the pulse rate, forms an electro-biometric subject signature, selects the enrolled electro-biometric signature template with the most similar pulse rate, and compares the new electro-biometric signature with the selected enrolled electro-biometric signature template.

In another preferred embodiment, the system uses signals acquired during long-term system operation to track possible variation in the enrolled subject electro-cardiologic signal and, if consistent changes occur, the enrolled signal is automatically adjusted to reflect these changes. This tracking process compensates for gradual changes in the electro-cardiologic signal over long time periods, but does not compensate for fast, acute changes

like those expected in connection with clinical heart conditions. In another embodiment, such acute changes may be reported to the subject indicating a need for medical consultation.

Second Aspect:

Biometric identification methods benefit from proper determination of an identification threshold. The identification threshold may be derived from correlation analysis between candidate signatures and registered database signatures. The threshold may be determined using a distribution of empirical data to achieve optimal identification performance. Yet a fixed threshold implicitly assumes deterministic signatures and stationary noise, while in practice signatures are variable and noise depends on mostly unpredictable external influences. Therefore, biometric identification methods, including those according to the first aspect, may be adversely affected by signal and noise variations in database and test readings. In general, this would yield decreased correlations for both matches and mismatches.

Thus, according to the second aspect, methods and systems of biometric identification, including those according to the first aspect, may use a dynamic threshold capable of compensating for the effect of signal variations and noise interference. This aspect yields a dynamic, data-dependent identification threshold. In the preferred embodiment, the dynamic threshold is re-calculated in each identification attempt using a statistical approach to normalize the correlation data and thus enable calculation of a quantifiable, statistically significant identification threshold. The threshold is shown to be resistant to variable signal and noise conditions.

The preferred method according to this second aspect is based on determination of a confidence limit for a correlation-based scoring between a test signature and a set of registered signatures. These ECG signatures can be empirically determined, but they may also be synthetic, in which case there is no need for a background database in the biometric matching process. Synthetic ECG signatures can be created by using random sets of reconstruction coefficients in the PCA-based ECG model. Alternately, reconstruction coefficient sets may be drawn according to a set of rules extracted from the distributions of real-life reconstruction coefficients derived from real subjects.

In any case, a confidence limit describes, with a given degree of statistical confidence, the upper and lower limits for the values in question. A two-tailed limit describes both upper and lower bounds, while a one-tailed limit describes only an upper or a lower cutoff, with the understanding that there is either no lower or no upper limit to the value of the variable. Confidence limits can be determined statistically, in several different ways, if the variable under consideration meets certain statistical criteria appropriate to each statistical method.

Most statistical methods rely on the values of a normally distributed variable, that is, according to the bell-shaped Gaussian distribution. Normally distributed variables have been well characterized statistically, and their statistical limits can be determined in a straightforward manner based on the variable average and variation.

When a variable is not distributed normally, a normalizing transformation may be used to transform the original variable into a new variable which would then be distributed normally, and may thus be used to determine

confidence limits. The appropriate mathematical transformation may be determined using statistical considerations, or by empirical examination of a sufficiently large dataset. In order to express the confidence limits in terms of the original variable, a back-transformation is also required.

Signal cross-correlation analysis may be used for the matching procedure. Values range from -1 (absolute negative correlation) through 0 (no correlation) to +1 (absolute positive correlation). Generally, significantly positive correlation indicates a probable true identification, and thus a one-tailed, upper confidence limit should be used to describe the dynamic identification threshold.

By definition, correlations are bounded variables and thus are not normally distributed. A mathematical transformation is necessary to normalize the correlation distribution allowing determination of the upper confidence limit. Alternatively, empirical techniques which do not rely on such transformations may be used.

A preferred method, described more fully below, is particularly appropriate for correlation analysis. It is based on the Fisher Z transformation, which converts correlations into a normally distributed variable.

Another method may use squared correlations. Since raw correlations are not additive, averages or other statistical functions of correlations have no statistical meaning. Squared correlations are additive, but they are also not normally distributed, so that additional transformations would be required. If prior processing of the correlations changes the distribution of their values, additional transformations may be necessary to account for these changes. These additional transformations include, but are not limited to, logarithms, squares, square roots, and transcendental functions.

Still another method would involve a degree of prior empirical testing, preferably where a large number of candidates are correlated to a large database. The likelihood of false identifications would be directly determined by examination of this database, or appropriate transformations could be empirically determined. However, because this method is not dynamic and must be performed prior to real testing, the effects of testing conditions cannot be easily compensated, requiring development of mathematical models for the influence of noise.

The preferred method according to this second aspect, the Fisher-transform method, involves transformation of the correlations between the candidate signature and the registered signatures in order to obtain a distribution of scores that are more nearly normally distributed. As noted above, data that meets assumptions of normality can be used to derive parametric confidence limits.

The Fisher Z transformation was designed to normalize correlations. The transformation may be expressed as follows:

$$Z_f = arctanh\ (r)$$

Where Z_f is the transformed value, ***arctanh*** is the hyperbolic arc tangent function, and ***r*** is the correlation. The ***arctanh*** should be expressed in radians.

Once all the correlations are transformed, a one-tailed confidence limit for the transformed scores may be determined by taking the mean of all the transformed correlations and the standard deviations of all the transformed correlations, with the exception of the candidate correlation, and calculating:

$$\text{Confidence limit} = tanh\ (Z_{f\ mean} + z^* sd_{Zf})$$

where ***z*** is the normal distribution **'z score'**, $\mathbf{Z_{f\ mean}}$ is the mean of transformed correlations with the database, and $\mathbf{sd_{Zf}}$ is the standard deviation of the transformed correlations with the data base.

The lower case z here refers to the value of the normal distribution **z-score**, which is derived based on the desired degree of confidence in the cut-off. A table of such scores is provided in **FIG. 10.**

In the table of **FIG. 10**, the standard deviation is multiplied by the appropriate z-score and is added to the mean, and the entire quantity back-transformed to a correlation by taking the hyperbolic tangent.

For example, a 95% confidence limit could be determined using a z score of 1.65. So if the mean of the transformed values was 0.05, and the standard deviation was 0.25, the 95% confidence limit would be 0.72. That is, a correlation value over 0.72 would only occur by chance less than 5% of the time.

A reverse procedure is used to determine the likelihood that any specific candidate identification is due to random chance. By solving for the z-score:

$$z = (Z_{fc} - Z_{f\ mean}) / sd_{Zf}$$

where ***z*** is the normal distribution **'z score'**, $\mathbf{Z_{fc}}$ is the transformed candidate correlation, $\mathbf{Z_{f\ mean}}$ is the mean of transformed correlations with the database, and $\mathbf{sd_{Zf}}$ is the standard deviation of the transformed correlations with the data base.

The resulting z-score can be converted to a 1-tailed probability value by reference to a table of the cumulative normal distribution, and interpolation if necessary. For example, with reference to the abbreviated table above, a z-score of 1.80 would suggest a 3.75% probability that the candidate correlated so highly by chance.

As mentioned above, if noise in the registered signatures or in the candidate signature is random, it would reduce the overall correlations with the candidate value. The true identification, if it exists, would therefore have a lower correlation with the candidate. It should be noted that variability of raw correlations increases as the raw values decrease, since high raw correlations are less variable due to a ceiling effect of maximum correlation of 1, but this is compensated for by the transformation. Thus, a dynamic threshold with the desired certainty may be re-calculated in each identification attempt using the foregoing methods. Importantly, overall random noise still tends to drive all correlations toward zero and reduce overall true variability, thereby lowering the confidence limit accordingly; yet a true match would remain significant as long as the signal to noise ratio does not fall below a certain limit.

The following examples of the second aspect are based on a 38-subject database. All subjects are healthy individuals, participating in the study on a voluntary basis.

Example 1: Normalization of Correlations

A set of 703 cross-correlations was obtained by correlating all pairs in the database. The raw and z-transformed correlation distributions are presented in **FIG. 11.** While raw correlations are not normally distributed (top), the transformed correlations appear to represent a near-normal distribution (bottom).

Example 2: Performance

The biometric identification method was implemented using analysis of 38 enrolled signatures and 38 test

signatures. **FIG. 12** presents FAR and FRR performance curves as a function of a static threshold, and **FIG. 13** presents the performance curves as a function of a dynamic threshold. Clearly, the dynamic threshold provides significantly superior results (eg. EER_{Static}=3%, $EER_{Dynamic}$=0%).

Third Aspect:

As described above, the dynamic identification threshold is a data-driven threshold, preferably re-calculated in each identification session to establish a confidence limit and substantiate a statistical significance of the identification process. Yet overall scores still decrease with the drop in signal quality due to background noise, lowering the dynamic threshold and thereby reducing identification confidence. This problem calls for assessment of signal quality in both enrollment and identification phases to facilitate high performance recognition.

The third aspect solves this problem by calculation of a Q value — a type of signal quality index. A quality of signal index Q is a quantitative description of the quality of the ECG signature. It is based on an analysis of the random error in two or more ECG complexes, derived with reference to their signal average ECG.

The Q value may be used to confirm signal quality during the enrollment and identification phases, ensuring adequate system performance. In case of a Q factor lower than required by a predefined threshold (itself based on the desired level of identification confidence) the measurement may either be extended or repeated until the confidence requirement is met.

One preferred methodology derives Q in a series of steps:

(1) The input ECG signal is segmented into ECG complexes comprised of the conventional wave morphology features (e.g. P, Q-R-S, T elements).

(2) The ECG complexes are aligned ("time-locked") relative to the R wave peak.

(3) An average ECG is derived from the aligned ECG complexes. The preferred method is to take an arithmetic mean, although other methods may be employed, such as the harmonic mean, geometric mean, weighted mean, or median. Other alternatives include transforming the original signals by other methods such as by Principal Component Analysis.

(4) Each original ECG complex is processed relative to the average ECG, such that some difference is derived against the average ECG. The preferred method is to perform subtraction, i.e. original ECG minus average ECG, although other methods may be employed (e.g. division of the original ECG by average ECG). If the average ECG is a stable and true representation of the subject's ECG, then the resulting difference is a representation of the noise inherent in each individual ECG complex (ECG noise).

(5) Each sample point which corresponds in time across each ECG noise complex is processed together to derive a measure of variability. The most preferred method is to determine the variance. Other measures that may be employed include standard deviation or range.

(6) An average is taken of these measures of variability. The most preferred method is to take an arithmetic average. Other methods may involve taking averages after transformation (e.g. log), or taking alternative averages (geometric, harmonic, median). Other summary scores may also be employed, such as the maximum.

Noting that the signal may be normalized prior to analysis, the average may itself be employed as a Q index,

as it is directly related to the SNR. Alternatively, various other scaling transformations may be applied to the average to convert it to an index with the desired minima, maxima, and linearity characteristics.

Example 1 according to the Third Aspect: Q (Signal Quality) vs. NSR (Noise to Signal Ratio)

If X denotes the ECG data matrix, each row representing one ECG complex may be denoted $x_i(n)$ where i is the index of an ECG complex and n represents a discrete time unit. The average of all ECG complexes is denoted $\underline{x}(n)$. For every point in time n we calculate the error term: $e_i(n)=x_i(n)-\underline{x}(n)$, whose variance shall be denoted: $\sigma_e^2(n)$. A preferred scaling conversion, transforming the average of variability into a zero to one range is defined as follows:

$$Q=(1+100*\ \underline{\sigma}_e^2(n))^{-0.5}$$

A simulation shown in **FIG. 14** demonstrates the utility of using the above Q factor to assess the signal to noise level. This simulation uses real-life ECG recordings with increasing levels of Gaussian white noise added to the signal. **FIG. 14** presents Q values as a function of the Noise to Signal Ratio (NSR). It can be seen that once Q starts to decline from its plateau, it drops monotonically with the increase in NSR, until the ECG alignment procedure breaks down (NSR ~ -35dB, Q ~ 0.2).

Example 2 according to the Third Aspect: Score as a function of Signal Quality

In theory, match scores close to 1 indicate a positive match, while non-match scores should tend to zero indicating complete lack of correlation. In practice, however, true match scores are influenced by temporal variations in the

ECG signature and, more significantly, from background noise. Thus, a higher signal quality is required for short time, high scored identification. It should be noted that high quality signal increases the upper bound on match score, but does not influence the lower bound which depends on the cardiologic signature variability. The example represented by **FIGS. 13** and **14** demonstrates score distribution as a function of signal quality, based on a database of 38 subjects. **FIG. 15** shows short data segments of 5 seconds each. In contrast, **FIG. 16** shows longer segments of 20 seconds each (**FIG. 16**). Obviously, with longer segments the effect of noise is compensated to some extent and the score distribution flattens.

Example 3 according to the Third Aspect: Signal Quality and Duration of Recording

Signal quality may be quantified using the Q parameter. With smaller Q values, and provided that Q does not fall below a certain limit where the ECG alignment process breaks down, longer recordings are necessary to maintain a certain level of statistical significance. **FIGS. 15** and **16** show the increase in identification score as a function of the length of recording for a given Q value.

Thus, according to this third aspect, the methods and systems disclosed herein may calculate signal quality using a Q-factor or other measure, and cause the system to seek a sample with reduced noise or to take a longer sample based on the Q-factor or other signal quality measure and the desired degree of identification confidence.

Fourth Aspect:

According to a fourth aspect, the methods and systems disclosed herein may encrypt stored signatures. This safety

feature is designed to prevent misuse of the data in the database notwithstanding that the various methods and systems herein typically operate on stored signatures rather than raw ECG data. Thus, an added layer of security may be employed by encrypting the signatures themselves. To that end, a variety of scrambling techniques may be used including the PKI (public key infrastructure) techniques used for credit card data. This fourth aspect makes improper use of the enrolled subject's data all the more difficult, since an unauthorized person would have to decrypt the signature and then still need to convert the signature back into a raw data signal, an impossible task without knowing which common features were removed from the raw data. Thus, one advantage of the systems and methods disclosed herein is that they make it extremely difficult for anyone to misuse the stored information.

Fifth Aspect:

Biometric identification systems are in general vulnerable to enrollment fraud. The systems and methods according to this fifth aspect solve this problem by using ECG data from genetically related individuals who have enrolled in the database. Immediate family members often have ECGs that share common features. By correlating a subject's signature with the general population and/or with those enrollees he or she is purportedly related to, the system can confidently determine whether or not the subject is who they purport to be. This technique can be used in addition to confirming the individual's identity through conventional methods such as picture identification and/or fingerprint matching. However, unlike those methods, which are non-Euclidian and not amenable to clustering based on similarity, this technique can determine fraud at any stage

of enrollment process by determining a probability of a genetic relationship based on the enrollee's ECG signature.

Sixth Aspect:

The systems and methods disclosed herein may also make use of ultra-high impedance probes to measure ECG. Since reliability and ease of use is important for an ECG-based biometric identification system, it is advantageous to measure an ECG at a single point, or even without touching the subject. Electric potential probes can work with biometric methods and systems, including those described herein, to increase reliability and ease of use for biometric identification. Ultra-high impedance probes come in a variety of forms. See e.g. Electric potential probes—new directions in the remote sensing of the human body, Harland et al., Meas. Sci. Technol. 13 (2002) 163-169. The ultra-high input impedance probes according to this aspect preferably have ultra-low noise characteristics, and do not require a current conducting path in order to operate. As a result, they work well with the foregoing methods and systems even when used by a layperson without the help of an expert system operator. Thus, these probes may be used in airport-based biometric identification systems, such as by acquiring an ECG signal when an individual passes through a scanner (similar to a metal detector) in full dress. Likewise, a single probe may be used to collect an ECG from an individual's finger tip, such as at an ATM or gaming machine. The use of a single probe contact gives the subject more freedom of movement and makes it easier for him or her to comply with the identification and enrollment regimen. This is particularly useful when the biometric identification systems described herein are used to control the subject's operation of machinery, especially when the

machine requires physical contact to operate (e.g., a firearm or vehicle). The single probe and remote probe ECG capture systems according to this aspect may also be complemented by noise reduction strategies to reduce body noise and EMG.

Seventh Aspect:

According to a seventh aspect, a biometric identification method and system may correlate the match scores for a subject (which are created by comparing the subject's signature with those of database enrollees) with the match scores of a plurality of enrollees (which are created by comparing the enrollees' signatures with those of database enrollees). Thus, rather than analyzing a distribution of a subject's correlated match scores, this identification technique analyzes the distribution of the correlation of a subject's match scores and those of the enrollees. As with the fifth aspect, the methods and systems according to this aspect are useful for identifying related individuals. This is because an individual related to a group of enrollees will have a Gaussian distribution of match scores that has a substantially higher median than a Gaussian distribution of the match scores for an individual unrelated to the enrollees. Thus, by examining the distribution of match scores, the probability of a subject's genetic relationship with the enrollees may be confirmed.

Eighth Aspect:

Finally, in the alternative or in addition to the correlation techniques described above, the methods and systems described herein may employ a weighted correlation for identification. According to this aspect, the correlation may give different weights to various signature

differences. For example, signature differences due to QRS complex features may be weighted more than signature differences due to T or P complex features. The systems and methods may also use the root mean square of the signature values as part of a weighting function since T is highly variable, QRS is stable, and P is somewhere in the middle. Thus, the signatures may be normalized using root-mean-square computations, L1 metrics or another normalizing technique.

Preferred Embodiment That May Be Used With All Aspects:

FIG. 19 shows a functional diagram of a preferred system. Likewise, **FIG. 20** shows a functional diagram of a preferred signal processor. The term "processor" is used herein generically and the processing may be done by physically discrete components, such as with co-processors on an IC chip, or the processor may comprise a physically integral unit.

General Example That May Be Used With All Aspects:
ENROLLMENT ALGORITHM

The following is an example algorithm for an enrollment phase that may be used with any of the foregoing aspects:

i. Let $x_i(n)$ represent a 20-second, 250Hz digitized sample of the i^{th} new subject, where n denotes discrete units of time.

ii. $x_i(n)$ is band-pass filtered in the range 4Hz – 40Hz.

iii. The filtered signal is denoted $y_i(n)$.

iv. The filtered signal $y_i(n)$ is searched for QRS complexes, identifying the 'R' peaks as anchor points.

v. The filtered signal $y_i(n)$ is maintained or inverted to obtain positive 'R' peaks.

vi. The identified QRS complexes are counted to establish an average pulse rate reading PR_i.

vii. The filtered signal $y_i(n)$ is segmented around the anchor points, taking 50 samples before and 90 samples after each 'R' anchor point.

viii. Each data segment is normalized by the amplitude of the 'R' anchor point.

ix. The segments are aligned around the anchor points and averaged to produce the subject electro-cardiologic signal, denoted $s_i(n)$.

x. The subject electro-cardiologic signal $s_i(n)$ is adjusted according to the average pulse rate PR_i, by normalizing 'P' and 'T' latencies according to the pulse rate. The adjusted electro-cardiologic signal is denoted $v_i(n)$.

xi. The pulse rate adjusted subject's electro-cardiologic signal $v_i(n)$ is added to the database and is introduced into a grand-average $T(n)$.

xii. A set of electro-biometric signatures Φ_i is constructed by subtraction of the grand-average $T(n)$ from each of the pulse rate adjusted electro-cardiologic signals stored in the system database.

EXAMPLE: RECOGNITION ALGORITHM

The following is an example an algorithm for the recognition phase:

i. Let $x_j(n)$ represent a 10-second, 250Hz digitized sample of the tested subject.

ii. $x_j(n)$ is band-pass filtered in the range 4Hz – 40Hz.

iii. The filtered signal is denoted $y_j(n)$.

iv. The filtered signal $y_j(n)$ is searched for the locations of QRS complexes, using the R peak as an anchor point.

v. The filtered signal $y_j(n)$ is maintained or inverted to obtain positive 'R' peaks.

vi. The identified QRS complexes are counted to establish an average pulse rate reading PR_j.

vii. The filtered signal $y_j(n)$ is segmented around the anchor points, taking 50 samples before and 90 samples after each anchor point.

viii. The segments are aligned around the anchor points and averaged to produce the subject electro-cardiologic signal, denoted $s_j(n)$.

ix. The subject electro-cardiologic signal $s_j(n)$ is normalized according to the average pulse rate PR_j. The pulse rate adjusted subject electro-cardiologic signal is denoted $v_j(n)$.

x. An electro-biometric signature σ_j is constructed by subtraction of the grand-average $T(n)$ from the pulse rate adjusted electro-cardiologic signal $v_j(n)$.

xi. The correlation coefficients between the electro-biometric signature σ_j and all the enrolled electro-biometric signatures Φ_i are calculated and squared, maintaining their original arithmetic sign.

xii. The largest sign-maintained squared correlation value is selected and compared to a preset threshold.

xiii. If the selected largest sign maintained squared correlation value is larger than the preset threshold then a positive match is indicated, and the subject is identified.

Thus, a method and apparatus of acquisition, processing, and analysis of electro-cardiologic signals for electro-biometric identity recognition may include any subset of the following enrollment and recognition steps:

ENROLLMENT

Acquisition, digitization, and storage of electro-cardiologic signals from subjects;

a. Formation of an electro-cardiologic signal database;

b. Partition of the template database into several subsets based on electro-cardiologic signal similarity;

c. Construction of one or more grand averages;

d. Derivation of subject-specific electro-biometric signatures.

RECOGNITION

VERIFICATION

The newly captured electro-biometric signature is compared with the subject specific enrolled electro-biometric signature template;

a. Correlation and confidence analysis of the newly captured subject electro-biometric signature with

the relevant stored electro-biometric signature template;

b. Display and registration of the recognition result and/or activation of a physical or virtual local/remote mechanism.

IDENTIFICATION

The newly captured electro-biometric signature is compared with all of the electro-biometric signature templates participating in the database;

a. Correlation and confidence analysis of the newly captured subject electro-biometric signature with all stored electro-biometric signature templates;

b. Display and registration of the recognition result and/or activation of a physical or virtual local/remote mechanism.

In a preferred embodiment, the E-BioID system measures an electrical bio-signal from the human body through conductive sensor plates. These same plates may be used for bidirectional interaction with the subject's nervous system, for example, by inducing a sympathetic skin response in the user with small magnitude electrical stimulation that is provided through the plates. Such bidirectional interaction constitutes a biological challenge-response mechanism that ensures submission of a fresh bio-signal without requiring active participation of the user in the challenge-response procedure.

Others may readily modify and/or adapt the embodiments herein for various applications without undue experimentation and without departing from the generic concept. Such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments. It is to be understood that the

phraseology or terminology employed herein is for the purpose of description and not of limitation. The means, materials, and steps for carrying out various disclosed functions may take a variety of alternative forms and still fall within the literal or equivalent scope of the claims.

Thus the expressions "means to..." and "means for...", or any method step language, as may be found in the specification above and/or in the claims below, followed by a functional statement, are intended to define and cover whatever structural, physical, chemical or electrical element or structure, or whatever method step, which may now or in the future exist which carries out the recited function, whether or not precisely equivalent to the embodiment or embodiments disclosed in the specification above, i.e., other means or steps for carrying out the same functions can be used; and it is intended that such expressions be given their broadest interpretation.

Claims

1. A method for identifying an individual, comprising:

producing and storing a first biometric signature that identifies a specific individual by forming the difference between a representation of the heartbeat pattern of the specific individual and a stored representation of common features of heartbeat patterns of a plurality of individuals;

after said producing step, obtaining a representation of the heartbeat pattern of a selected individual and producing a second biometric signature by forming the difference between the heartbeat pattern of the selected individual and the stored representation of the common features of the heartbeat patterns of the plurality of individuals; and

comparing said second biometric signature with said first biometric signature to determine whether the selected individual is the specific individual.

2. The method of claim 1 wherein:

said step of producing and storing comprises producing and storing a plurality of first biometric signatures, each identifying a respective individual, by forming the difference between a representation of the heartbeat pattern of each respective individual and the stored representation of the common features of the heartbeat patterns; and

said step of comparing is carried out with respect to each of said first biometric signatures.

3. The method of claim 2 comprising the preliminary step of obtaining representations of the heartbeat patterns of a plurality of individuals, and deriving and storing the representation of the common features of the heartbeat patterns of a plurality of individuals from at least a selected number of the representations.

4. The method of claim 3 wherein said step of deriving and storing the representation of the common features of the heartbeat patterns of a plurality of individuals comprises deriving and storing a plurality of representations of the common features of the heartbeat patterns each from a respectively different group of the plurality of individuals.

5. The method of claim 3; wherein said step of deriving and storing the representation of the common features of the heartbeat patterns of a plurality of individuals comprises producing an average of the heartbeat patterns of the plurality of individuals.

6. The method of claim 3, wherein said step of deriving and storing the representation of the common features of the heartbeat patterns of a plurality of individuals comprises performing one of principal component analysis or wavelet decomposition.

7. The method of claim 2 wherein said step of comparing comprises correlating said second biometric signature with each of said first biometric signatures and identifying that one of said first biometric signatures that correlates most closely to said second biometric signature.

8. The method of claim 7, wherein said step of correlating comprises obtaining a correlation coefficient associated with each first biometric signature, and said step of comparing further comprises comparing the correlation coefficient associated with the identified first biometric signature with a correlation coefficient threshold.

9. The method of claim 1 wherein said step of comparing comprises: correlating said second biometric signature with said first biometric signature to obtain a correlation coefficient; and comparing the correlation coefficient associated with the identified first biometric signature with a correlation coefficient threshold.

10. The method of claim 1 wherein said step producing and storing a first biometric signature comprises storing the signature in a local database.

11. The method of claim 1 wherein said step producing and storing a first biometric signature comprises storing the signature in a remote database.

12. The method of claim 1 wherein said step of obtaining a representation of the heartbeat pattern of a selected individual comprises compensating for deviations in the pulse rate of the selected individual from a selected pulse rate.

13. The method of claim 1 wherein said step of obtaining a representation of the heartbeat pattern of a selected individual comprises obtaining several representations of heartbeat patterns.

14. The method of claim 1 wherein said step of producing and storing a first biometric signature of a specific individual comprises obtaining a plurality of representations of the heartbeat pattern of the specific individual over a period of time and producing successive first biometric signatures each from a respective one of the plurality of representations of the heartbeat pattern of the specific individual.

15. Apparatus for identifying an individual, comprising:

means for producing and storing a first biometric signature that identifies a specific individual by forming the difference between a representation of the heartbeat pattern of the specific individual and a stored representation of common features of the heartbeat patterns of a plurality of individuals;

means for obtaining, after the first biometric signature has been produced and stored, a representation of the heartbeat pattern of a selected individual and producing a second biometric signature by forming the difference between the heartbeat pattern of the selected individual and the stored representation of the common features average of the heartbeat patterns of the plurality of individuals; and

means for comparing said second biometric signature with said first biometric signature to determine whether the selected individual is the specific individual.

16. The apparatus of claim 15 wherein:

said means for producing and storing comprises means for producing and storing a plurality of first biometric signatures, each identifying a respective individual, by forming the difference between a representation of the

heartbeat pattern of each respective individual and the stored representation of the common features of the heartbeat patterns; and

said means for comparing is carried out with respect to each of said first biometric signatures.

17. The apparatus of claim 16 wherein said means for producing and storing comprises means for obtaining representations of the heartbeat patterns of a plurality of individuals, and means for deriving the stored representation of the common features from at least a selected number of the representations.

18. The apparatus of claim 17 wherein said means for deriving comprises means for deriving a plurality of stored representations of the common features, each from a respectively different group.

19. The apparatus of claim 16 wherein said means for comparing comprises means for correlating said second biometric signature with each of said first biometric signatures and identifying that one of said first biometric signatures that correlates most closely to said second biometric signature.

20. The apparatus of claim 19, wherein said means for correlating comprises means for obtaining a correlation coefficient associated with each first biometric signature, and said means for comparing further comprises means for comparing the correlation coefficient associated with the identified first biometric signature with a correlation coefficient threshold.

21. The apparatus of claim 15 wherein said means for comparing comprises: means for correlating said second biometric signature with said first biometric signature to obtain a correlation coefficient; and means for comparing the correlation coefficient associated with the identified first biometric signature with a correlation coefficient threshold.

22. The apparatus of claim 15 wherein said apparatus is one of: a smart card; a passport; a driver's license apparatus; a Bio-logon identification apparatus; a palm pilot; a cellular embedded identification apparatus; an anti-theft apparatus; an ECG monitoring apparatus, an e-banking apparatus, an e-transaction apparatus; a pet identification apparatus; a physical access apparatus; a logical access apparatus; an apparatus combining ECG and Fingerprint monitoring; and an apparatus combining ECG signature comparison and any other form of biometric analysis.

23. The apparatus of claim 15 wherein said apparatus is a Bio-logon identification apparatus for remote logon to secure resources.

24. The apparatus of claim 15 wherein said apparatus is continuously in operation.

25. The apparatus of claim 15 wherein said means for obtaining are constructed to be contacted by either the hands or feet of the selected individual.

26. The apparatus of claim 15 wherein said apparatus is provided in a smart card that is enabled for a limited

period of time after successful recognition and disabled thereafter until the next successful recognition is performed.

27. The apparatus of claim 15 wherein said apparatus is constructed to operate with encryption keys or digital signatures.

28. The apparatus of claim 15 incorporated into a watch worn on the wrist, where the signal is measured between the wrist on which the watch is worn and the other hand of the wearer.

29. A biometric identification system comprising

a) an ECG signal acquisition module;

b) an ECG signal processor wherein said signal processor comprises an ECG signature template generator; and

c) an output module.

30. The biometric identification system of Claim 29 wherein said ECG signature template generator has an analytical ECG model input which it uses to remove common features from one or more ECG components of an ECG signal provided by said ECG signal acquisition module.

31. The biometric identification system of Claim 29 further comprising an enrolled signature database, divided into subsets, wherein said ECG signature template generator uses at least one said database subset to remove common features from one or more ECG components of an ECG signal provided by said ECG signal acquisition module.

32. A biometric identification system comprising

a) an ECG signal acquisition module;

b) an enrolled signature database;

c) a signal processor that further comprises an ECG signature generator, and a signature comparator that compares an ECG signature with at least one enrolled ECG signature; and

d) an output module.

33. The biometric identification system of Claim 32 wherein said comparator is a closed search comparator.

34. The biometric identifications system of Claim 32 wherein said signature comparator is a signature correlation analyzer.

35. A biometric identification system comprising

a) a signal acquisition module;

b) an enrolled signature database;

c) a signal processor that comprises an ECG signature generator, a signature comparator that compares one or more ECG signatures generated by said ECG signature generator with a plurality of enrolled ECG signatures from said enrolled signature database, a match score generator that outputs a series of match scores based on the output of said signature comparator, and a match score correlator that correlates said match scores for said one or more ECG signatures with the match scores for at least one enrolled signature; and

d) an output module.

36. A biometric identification system comprising

a) a signal acquisition module;

b) a signal processor that further comprises an ECG signature generator, and a signature comparator which

comprises a fuzzy logic analyzer to compare at least one ECG signature with at least one enrolled ECG signature;

c) an output module.

37. A biometric identification system comprising

a) a signal acquisition module;

b) a signal processor that further comprises

i) an ECG signature generator,

ii) a signature comparator,

iii) and a dynamic threshold generator; and

c) an output module.

38. The biometric identification system of Claim 37 wherein said signature comparator is a signature correlator.

39. A biometric identification system comprising

a) a signal acquisition module;

b) a signal processor that further comprises

i) an ECG signature generator,

ii) a signature correlator, and

iii) a dynamic threshold generator wherein said generator comprises a correlation transformer; and

c) an output module.

40. The biometric identification system of Claim 39 wherein said correlation transformer is a Z-score generator.

41. The biometric identification system of Claim 39 wherein said correlation transformer is a squared correlation transformer.

42. A biometric identification system comprising

a) a signal acquisition module;

b) a signal processor that further comprises

i) an ECG signature generator,

ii) a signature correlator, and

iii) a signature quality calculator; and

c) an output module.

43. The biometric identification system of Claim 42 wherein said signal quality calculator comprises a Q-value generator.

44. The biometric identification system of Claim 43 wherein said signal quality calculator is connected to said signal acquisition module such that a low quality signal calculation causes the acquisition module to use a longer acquisition period.

45. The biometric identification system of Claim 43 wherein said signal quality calculator is connected to said output module in such a manner that a low quality signal calculation causes the output module to indicate that a new signal acquisition with reduced noise is needed.

46. A biometric identification system comprising

a) an ECG signal acquisition module;

b) an enrolled signature database;

c) a signal processor that comprises an ECG signature generator, a signature comparator that compares one or more ECG signatures generated by said ECG signature generator with a plurality of enrolled ECG signatures from said enrolled signature database;

d) a signature encryption module; and

e) an output module.

47. The biometric identification system of Claim 46 wherein said signature encryption module comprises a scrambler that uses a public key infrastructure technique.

48. A biometric identification system comprising

a) a signal acquisition module wherein said module comprises ultra-high input impedance probes;

b) an ECG signal processor that further comprises a ECG signature generator and a signature comparator; and

c) an output module.

49. The biometric identification system of Claim 48 wherein said ultra-high input resistance probes have ultra-low noise characteristics.

50. A biometric identification system comprising

a) a signal acquisition module;

b) a signal processor that further comprises an ECG signature generator, an ECG signature correlator, and a signature correlation weighting mechanism; and

c) an output module.

51. A lock comprising

a) a signal acquisition module;

b) an ECG signal processor that further comprises an ECG signature generator and a ECG signature comparator; and

c) a locking mechanism.

52. A room access control device comprising

a) a signal acquisition module;

b) an ECG signal processor that further comprises an ECG signature generator and an ECG signature comparator; and

c) a room access control.

53. A biometric identification system comprising

a) an ECG signal acquisition module;

b) a signal processor that further comprises a pulse rate normalization module; and

c) an identification output module.

54. The biometric identification system of Claim 53 wherein said ECG signal processor is a digital signal processor.

55. The biometric identification system of Claim 53 wherein at least one said ECG signal processor is integral to another apparatus.

56. The biometric identification system of Claim 53 wherein said signal acquisition module, said signal processor and said signal output module are part of an integral device.

57. A method for identifying an individual, comprising:

producing and storing a first biometric signature that identifies a specific individual by forming the difference between a representation of the heartbeat pattern of the specific individual and an analytical representation of common features of heartbeat patterns;

after said producing step, obtaining a representation of the heartbeat pattern of a selected individual and producing a second biometric signature by forming the difference between the heartbeat pattern of the selected individual and an analytical representation of the common features of the heartbeat patterns; and

comparing said second biometric signature with said first biometric signature to determine whether the selected individual is the specific individual.

58. A method of biometric identification comprising the steps of:

a) acquiring a first ECG signal;

b) processing said first ECG signal to generate an ECG signature template;

c) acquiring a second ECG signal;

d) processing said second ECG signal to generate an ECG signature;

e) comparing said ECG signature with said ECG signature template; and

f) outputting the result of said comparison.

59. The method of Claim 58 wherein said step of generating an ECG signature template removes common features of one or more ECG components from said ECG signal by subtracting common features of one or more ECG components provided by an analytical ECG model.

60. The method of Claim 58 further comprising the steps of g) creating a database of such ECG signature templates, h) dividing the ECG signature templates into subsets, and i) using at least one database subset to remove common features of one or more ECG components from an ECG signal.

61. A method of biometric identification comprising the steps of:

a) acquiring a first ECG signal;

b) processing said first ECG signal to generate an ECG signature template;

c) storing said ECG signature templates in an enrolled signature database;

d) repeating steps a) through c);

e) acquiring a second ECG signal;

f) processing said second ECG signal to generate an ECG signature;

g) comparing said second ECG signature with at least one enrolled ECG signature; and

h) outputting the result of said comparison.

62. The method of Claim 61 wherein said comparing step only compares said ECG signature with a single enrolled ECG signature.

63. The method of Claim 61 wherein said comparison step correlates said ECG signature with a plurality of enrolled signatures.

64. A method of biometric identification comprising the steps of:

a) acquiring an ECG signal;

b) processing said ECG signal to generate an enrolled signature database;

c) placing the resulting ECG signatures in a database;

d) repeating steps a) through c);

e) comparing one or more ECG signatures with a plurality of enrolled ECG signatures;

f) generating a series of match scores based on the results of said comparison step;

g) correlating said match scores for said one or more ECG signatures with the match scores for at least one enrolled signature; and

h) outputting the correlation results.

65. A method of biometric identification comprising:

a) acquiring an ECG signal;

b) creating an ECG signature from said ECG signal;

c) comparing said ECG signature with at least one enrolled ECG signature using fuzzy logic; and

d) outputting the result of said comparison.

66. A method of biometric identification comprising the steps of:

a) acquiring an ECG signal;

b) processing said ECG signal to generate an ECG signature;

c) comparing said ECG signature with a plurality of enrolled ECG signatures;

d) generating a dynamic threshold for said comparison; and

e) outputting the identification result.

67. The method of biometric identification system of Claim 66 wherein said step of signature comparison correlates said signatures.

68. A method of biometric identification system comprising the steps of:

a) acquiring an ECG signal;

b) processing said ECG signal to generate an ECG signature;

c) correlating said ECG signature with a plurality of enrolled ECG signatures;

d) transforming one or more of said correlations;

e) generating a dynamic threshold for said correlation; and

f) outputting the identification result.

69. The method of biometric identification system of Claim 68 wherein the step of transforming one ore more said correlations is used to generate a Z-score.

70. The method of biometric identification of Claim 68 wherein said step of transforming said one or more correlations squares said one or more correlations.

71. A method of biometric identification comprising the steps of:

a) acquiring an ECG signal;

b) calculating the quality of said signal;

c) processing said ECG signal to generate an ECG signature;

d) correlating said ECG signature with one or more enrolled ECG signatures;

e) comparing the result of said correlation step with a threshold; and

f) outputting the result of said comparison.

72. The method of biometric identification system of Claim 71 wherein said step of calculating signal quality calculates a Q-value.

73. The method of biometric identification system of Claim 71 further comprising the step of adjusting the time of acquisition based on the quality of the signal.

74. The method of biometric identification system of Claim 71 further comprising the step of acquiring a new signal in response to the signal quality calculation.

75. A method of biometric identification comprising the steps of:

a) acquiring a first ECG signal;

b) processing said ECG signal to generate an ECG signature;

c) encrypting said signature;

d) adding said encrypted signature to an enrolled signature database;

e) acquiring a second ECG signal;

f) processing said ECG signal to generate a second signature; and

g) comparing said second signature with one or more of said enrolled signatures in said enrolled signature database.

76. The method of biometric identification system of Claim 75 wherein said signature encryption step scrambles the signature using a public key infrastructure technique.

77. A method of biometric identification comprising the steps of:

a) acquiring an ECG signal using ultra-high input impedance probes;

b) processing said ECG signal to generate an ECG signature;

c) comparing said signature with at least one enrolled signature in an enrolled signature database; and

d) outputting the result of said comparison.

78. The biometric identification system of Claim 77 wherein said ultra-high input resistance probes have ultra-low noise characteristics.

79. A method of biometric identification comprising the steps of:

a) acquiring an ECG signal;

b) processing said signal to generate an ECG signature;

c) correlating said ECG signature with at least one ECG signature template in an enrolled signature database;

d) weighting the results of said signature correlation;

e) comparing the result of said weighted correlation with a threshold; and

f) outputting the results of said comparison.

80. A method of locking a security device comprising the steps of:

a) acquiring an ECG signal;

b) processing said ECG signal to generate an ECG signature;

c) comparing said ECG signature with one or more ECG signature templates in an enrolled signature database;

d) comparing the result of said comparison with an identification threshold; and

e) affecting a locking mechanism based on said comparison.

81. A method of controlling room access comprising the steps of:

a) acquiring an ECG signal;

b) processing said ECG signal to generate an ECG signature;

c) comparing said ECG signature with one or more ECG signature templates in an enrolled signature database;

d) comparing the result of said comparison with an identification threshold; and

e) permitting or denying room access based upon said comparison.

82. A method of biometric identification comprising the steps of:

a) acquiring an ECG signal;

b) processing said signal by normalizing it for pulse rate;

c) generating an ECG signature;

d) correlating said ECG signature with at least one ECG signature template from a signal taken at the normalized pulse rate or normalized for pulse rate;

e) comparing the result of said correlation with a threshold; and

f) outputting the result of said comparison.

83. The method of biometric identification system of Claim 82 wherein said processing step processes said signal digitally.

84. The method of biometric identification of Claim 82 further comprising the step of obtaining a non-ECG biometric reading.

85. The method of biometric identification system of Claim 84 further comprising the step of evaluating said non-ECG biometric reading and said outputted comparison result to identify an individual.

86. The method of biometric identification of Claim 1 further comprising the step of obtaining a non-ECG biometric reading.

87. The apparatus of Claim 15 further comprising a credit card that is enabled for a limited period of time after a positive identification and disabled thereafter until the next successful positive identification is performed.

88. The apparatus of Claim 15 further comprising a non-ECG biometric acquisition module.

89. The apparatus of Claim 29 further comprising a non-ECG biometric acquisition module.

90. An age analyzer comprising:

a) an ECG acquisition module;

b) an ECG signal processor;

c) a processed ECG signal comparator; and

d) an age analysis output module.

91. The analyzer of Claim 90 wherein said ECG signal processor comprises a signature generator and said processed signal comparator is a signature comparator.

92. The analyzer of Claim 90 wherein said processed ECG comparator compares the width of a subject's QRS complex with the width of a QRS complex signal template.

93. The analyzer of Claim 90 wherein said output module outputs its output over the Internet.

94. A method of age detection comprising the steps of:

a) acquiring an ECG signal;

b) processing said ECG signal;

c) comparing said processed ECG signal with one or more reference signals;

d) controlling access to an Internet Website based on the result of said comparison step.

95. The method of age detection of Claim 94 wherein said comparison step compares an ECG signature with one or more ECG signature templates.

96. The method of age detection of Claim 94 wherein said comparison step compares the width of a QRS signal complex with the width of one or more reference signal QRS complexes.

97. A biometric identification system comprising

a) an ECG signal acquisition module;

b) an enrolled signature database;

c) an ECG signal processor comprising an ECG signature generator that removes characteristic waveforms, which represent common ECG features of a group of individuals, from the ECG signal acquired by the ECG signal acquisition module;

d) an ECG signature comparator that compares an ECG signature with at least one enrolled ECG signature; and

e) an output module.

98. The system of claim 97 wherein said ECG signature generator removes characteristic waveforms representing the first principal components derived from a PCA of said group's ECG signals.

99. The system of claim 98 wherein said characteristic waveforms are weighted to approximate the extent of those characteristic waveforms present in the ECG signal acquired by the ECG signal acquisition model.

100. The system of claim 99 wherein said ECG signature generator removes said approximation from the ECG signal acquired by the ECG signal acquisition module.

101. The system of claim 98 wherein said ECG signal acquisition module acquires an ECG signal from an individual who is not a member of said group of individuals.

102. The system of claims 97, 98 and 99 wherein said characteristic waveforms are derived from synthetic ECGs.

103. The system of claim 97 wherein said ECG signature generator removes characteristic waveforms derived from an ICA of said group's ECG signals.

104. The system of claim 97 wherein said ECG signature generator removes characteristic waveforms derived from a WD of said group's ECG signals.

105. The system of claim 99 wherein said system uses reconstruction coefficients to weight said characteristic waveforms.

106. The system of claims 97, 98 and 99 wherein said ECG acquisition module comprises a bidirectional interface that provides for a biological challenge-response mechanism that does not require a conscious response from the user.

107. The system of claim 106 wherein said bidirectional interface comprises a conductive medium.

108. The system of claim 107 wherein said conductive medium is incorporated into an apparel item.

109. A method for identifying an individual comprising the steps of:

a) acquiring a subject's ECG;

b) decomposing ECGs from a group of individuals to determine a set of characteristic waveforms that represent common features of the group;

c) processing said subject's ECG by removing said characteristic waveforms; and

d) using the subject's processed ECG to identify the subject.

110. The method of claim 109 wherein the subject is not a member of said group of individuals.

111. The method of claim 109 wherein said decomposed ECGs are synthetic.

112. The method of claim 109 wherein said steps are performed in the listed order.

113. The method of claim 109 further comprising the step of weighting said characteristic waveforms to

approximate the extent of common features present in the subject's ECG.

114. The method of claim 113 wherein the step of removing said characteristic waveforms is accomplished by removing said approximation.

115. The method of claim 113 wherein said decomposing step is performed by applying PCA to the ECGs from the group of individuals, and said weighting step is performed by determining reconstruction coefficients for the principal components that represent common features so as to approximate the extent of said characteristic waveforms present in the subject's ECG.

116. The method of claim 115 wherein said approximation is removed from the subject's ECG.

117. The method of claim 115 wherein the principal components representing common features are time shifted to determine said reconstruction coefficients.

118. The method claim 109 wherein said decomposing step is ICA.

119. The method of claim 109 wherein said decomposing step is WD.

120. The method of claims 109, 110, 111 and 112 further comprise the step of challenging the subject in a way that does not require the subject's conscious response.

121. The method of claim 120 wherein the challenge step includes providing an electrical stimulus through a

conductive medium that is also used to acquire the subject's ECG.

122. A method of biometric identification comprising the steps of:

a) acquiring an ECG signal;

b) processing said ECG signal to generate an ECG signature;

c) correlating said ECG signature with a plurality of synthetic ECG signatures;

d) transforming one or more of said correlations;

e) generating a dynamic threshold for said correlation; and

f) outputting the identification result.

123. The method of claim 122 wherein the steps are performed in the listed order.

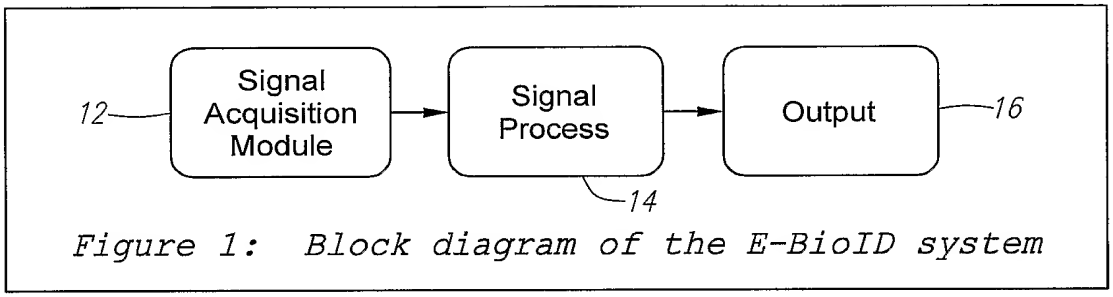


Figure 1: Block diagram of the E-BioID system

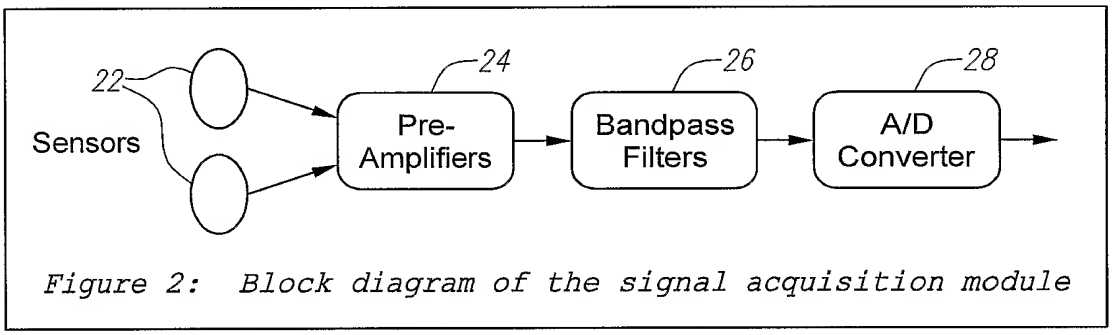


Figure 2: Block diagram of the signal acquisition module

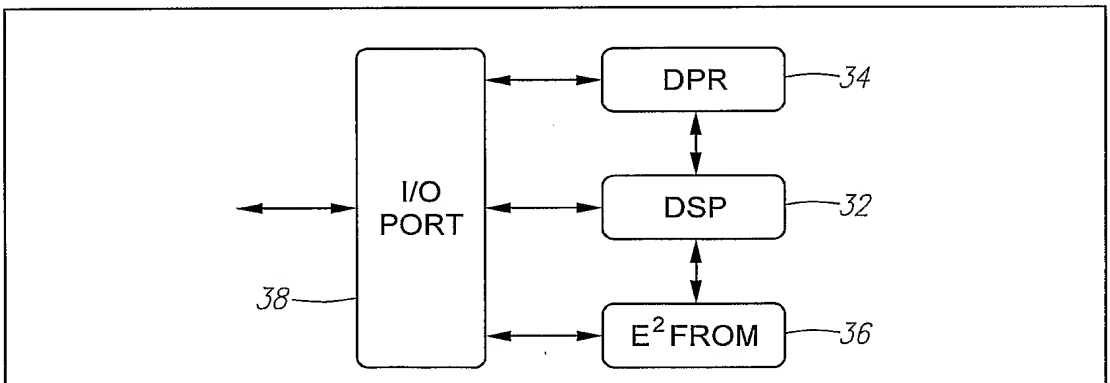
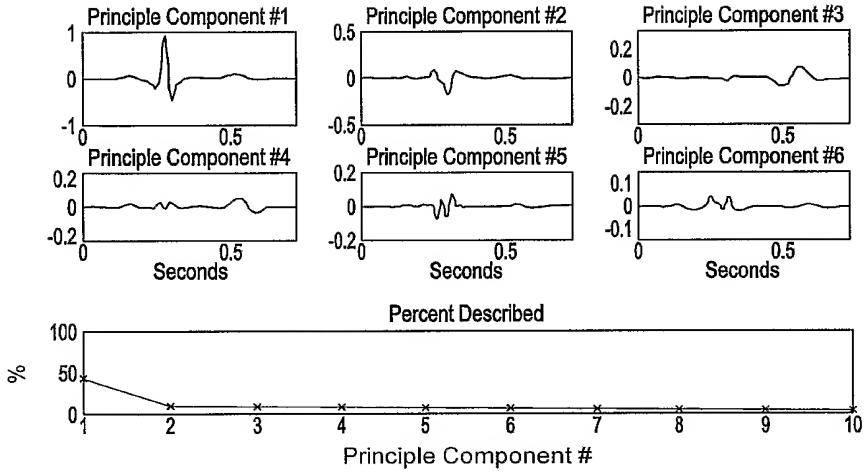
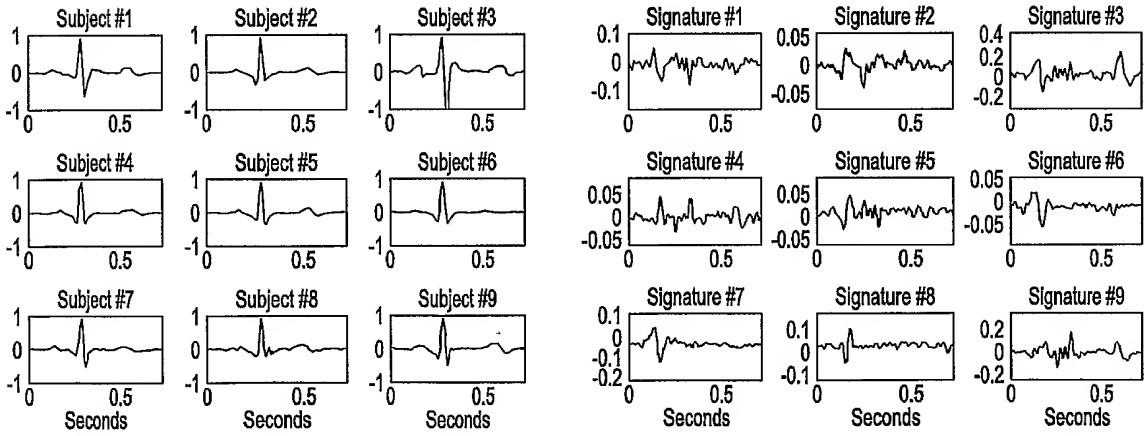


Figure 3: Block diagram of the sig. proc. module



THE MOST INFLUENTIAL 6 PCs (top)
RELATIVE CONTRIBUTION OF THE MOST INFLUENTIAL 10 PCs (bottom)

FIG. 4



ORIGINAL ELECTROCARDIOGRAPHIC SIGNALS (LEFT)
COMMON-ELIMINATED DERIVED SIGNATURES (RIGHT)

FIG. 5

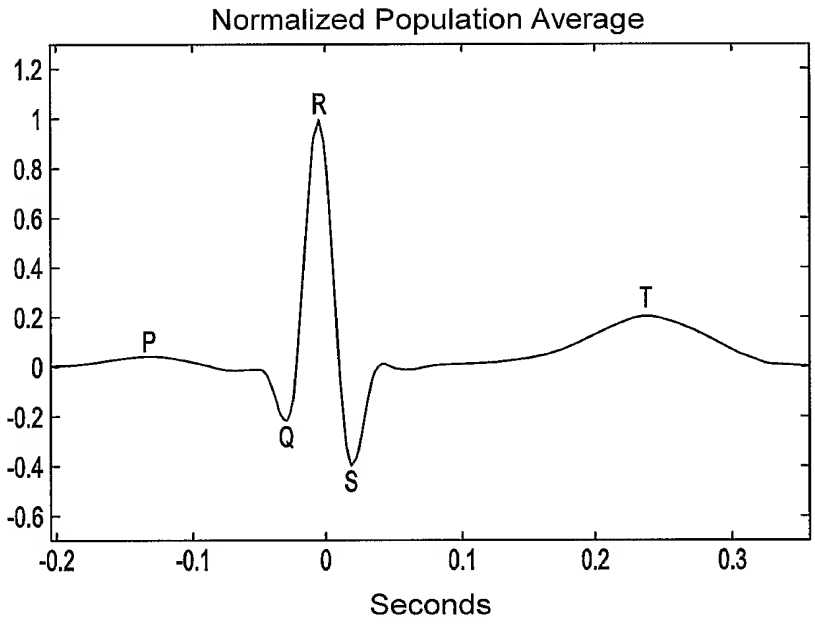


Figure 6: Normalized grand-average

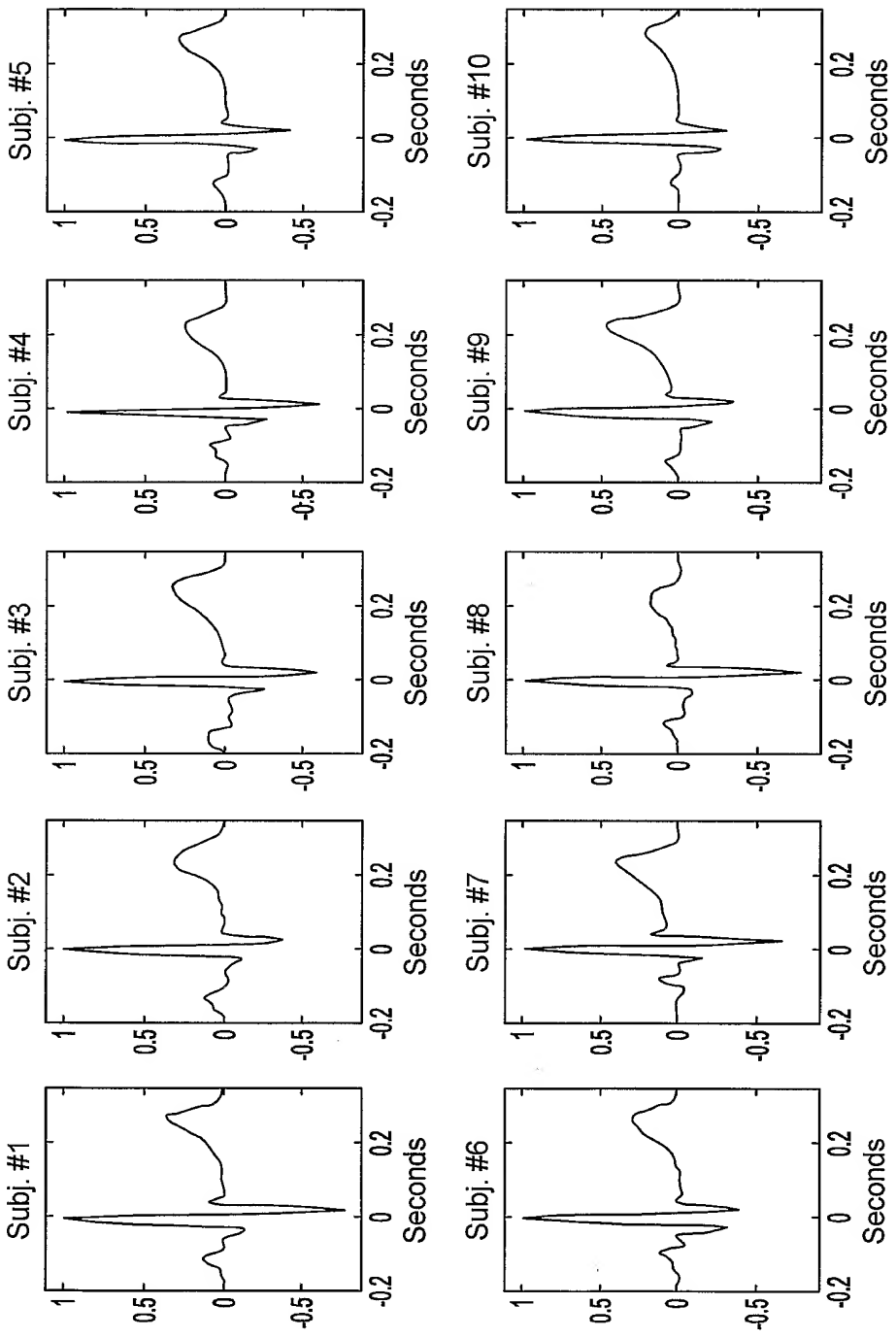


Figure 7: Electro-cardiologic signals of ten subjects

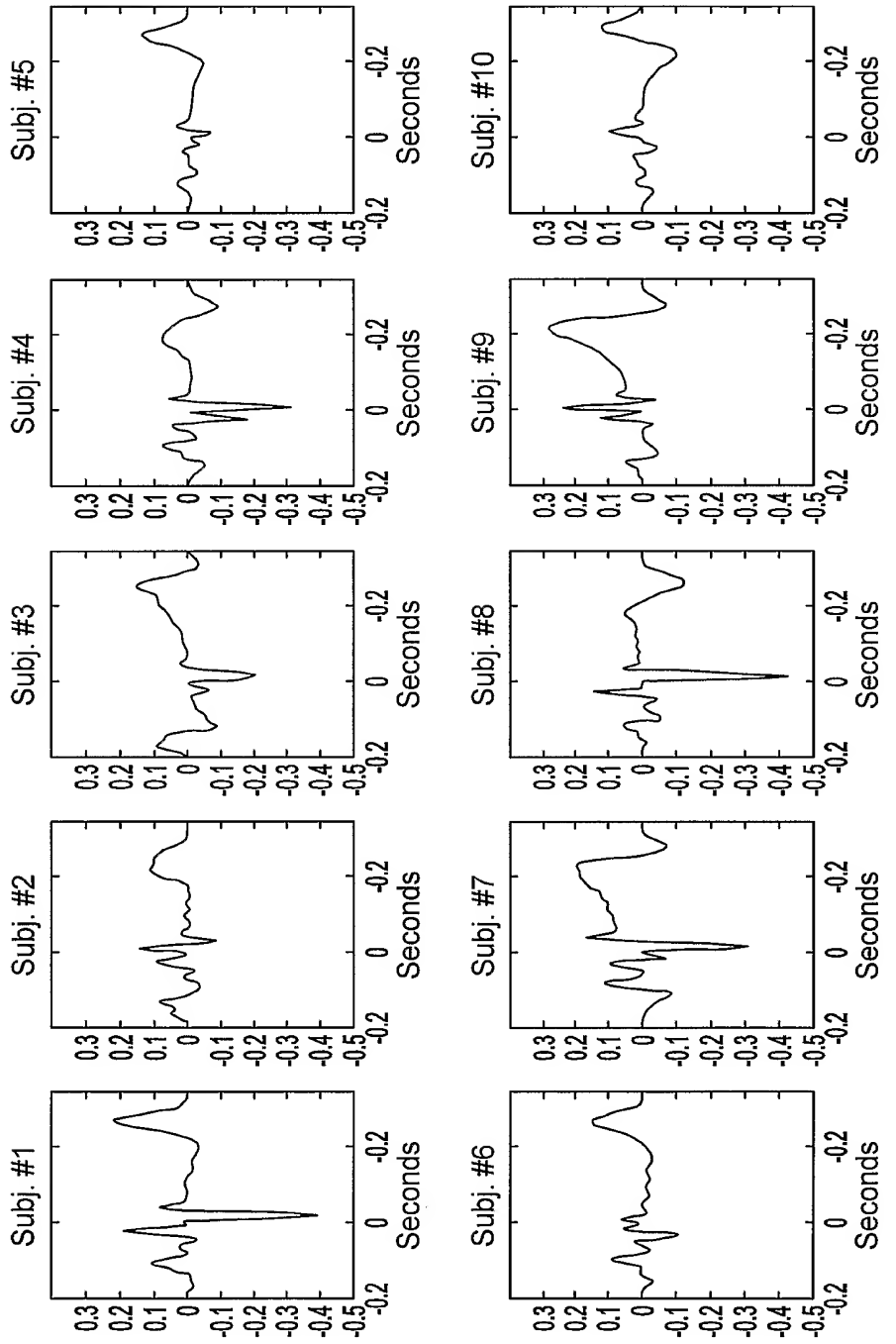


Figure 8: Signature templates of the above ten subjects

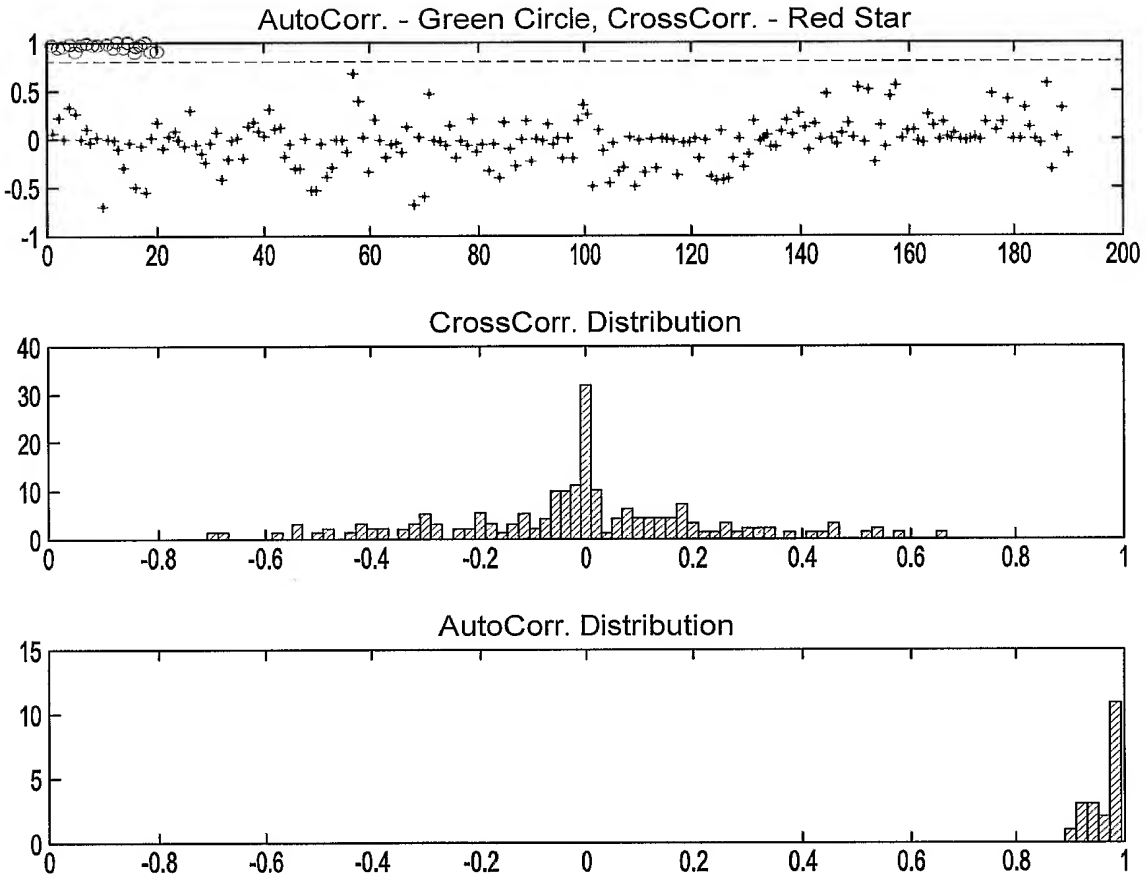


Figure 9: Distributions of correlation data

1-tailed limit	Unlikelihood	z score
99.99%	0.01%	3.71
99.90%	0.10%	3.09
99.50%	0.50%	2.58
99.00%	1.00%	2.33
97.50%	2.50%	1.96
95.00%	5.00%	1.65
90.00%	10.00%	1.28

Figure 10

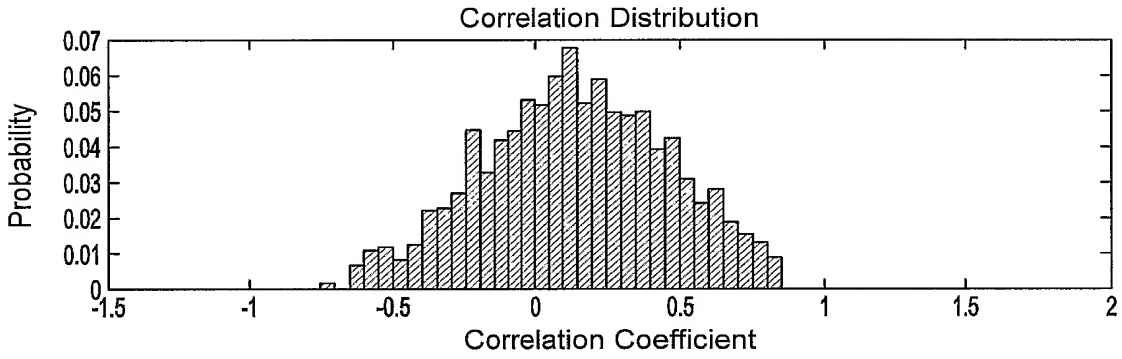


Figure 11A

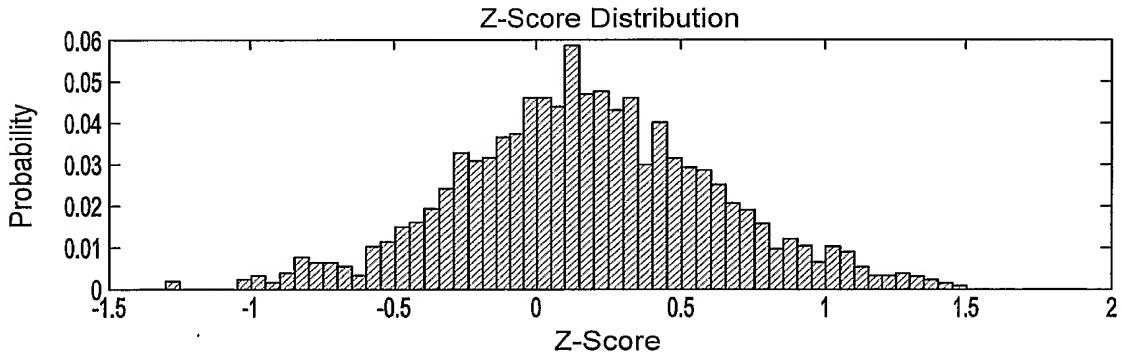


Figure 11B

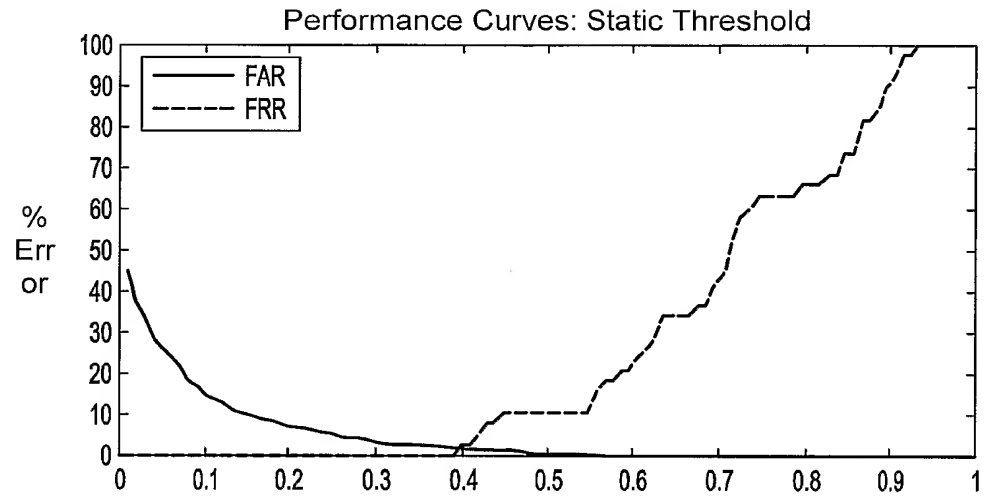


Figure 12: Identification Performance Curves (Static)

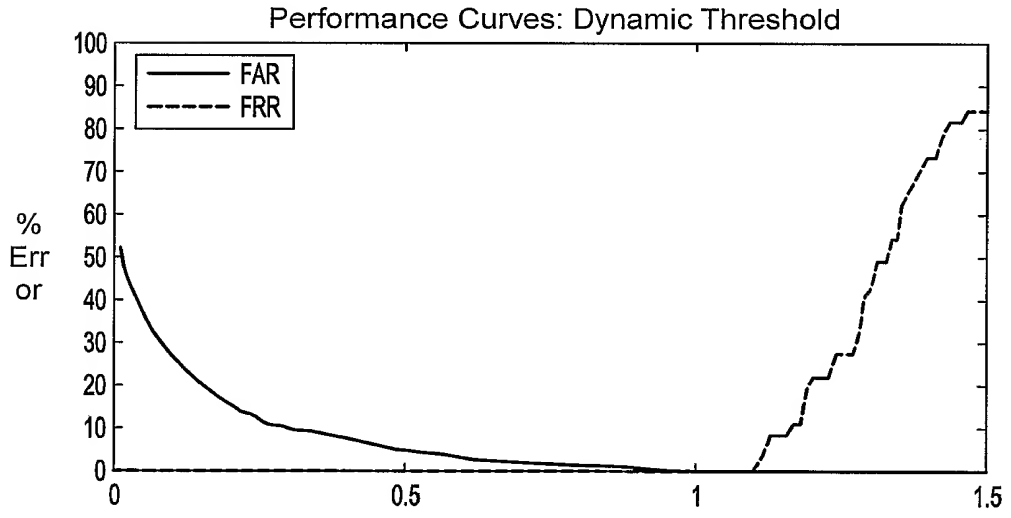


Figure 13: Identification Performance Curves (Dynamic)

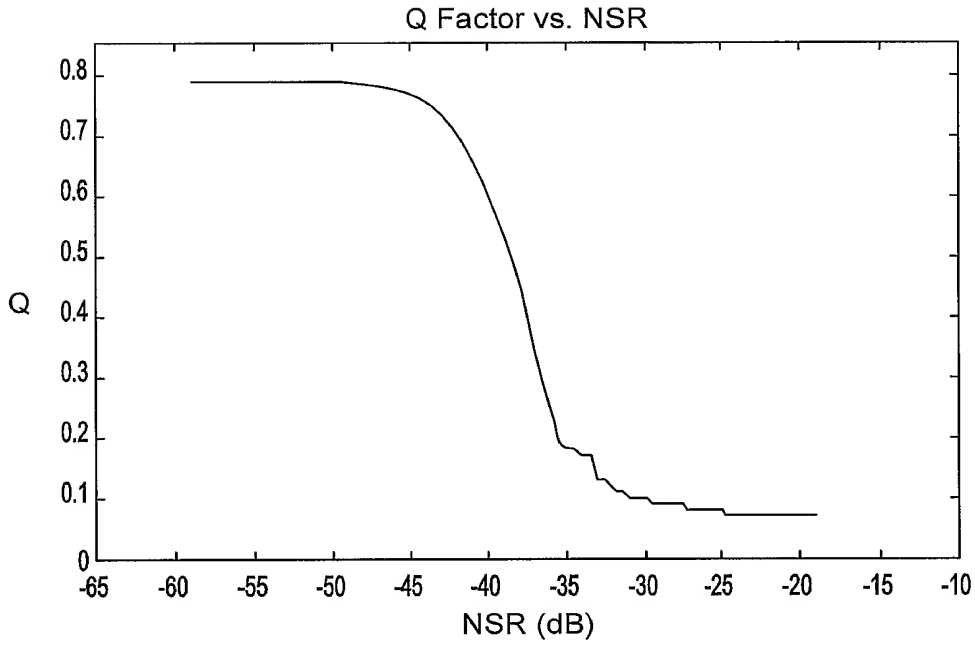


Figure 14: Signal Quality as a function of NSR

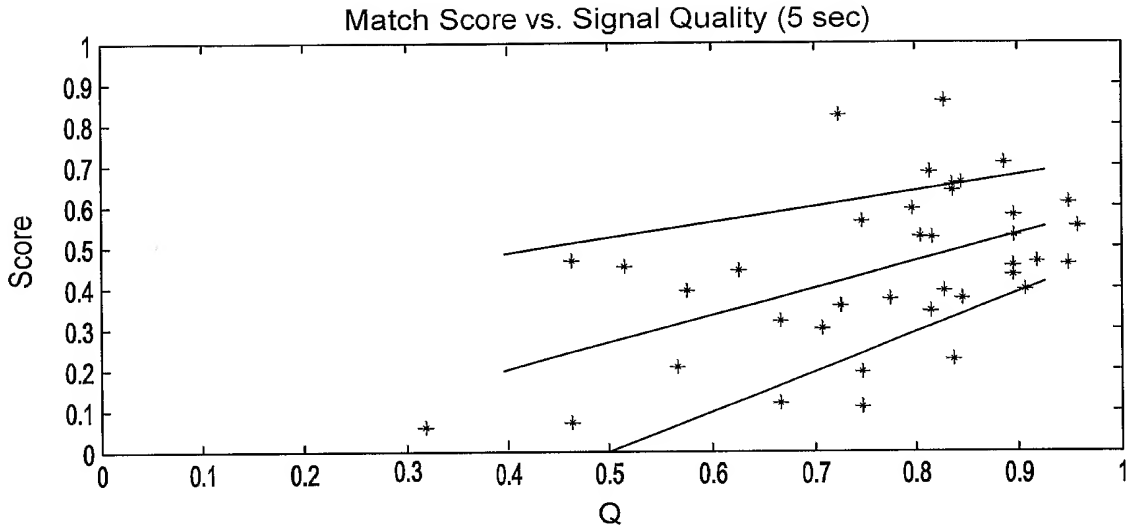


Figure 15: Match score distribution as a function of signal quality (5 sec segments)

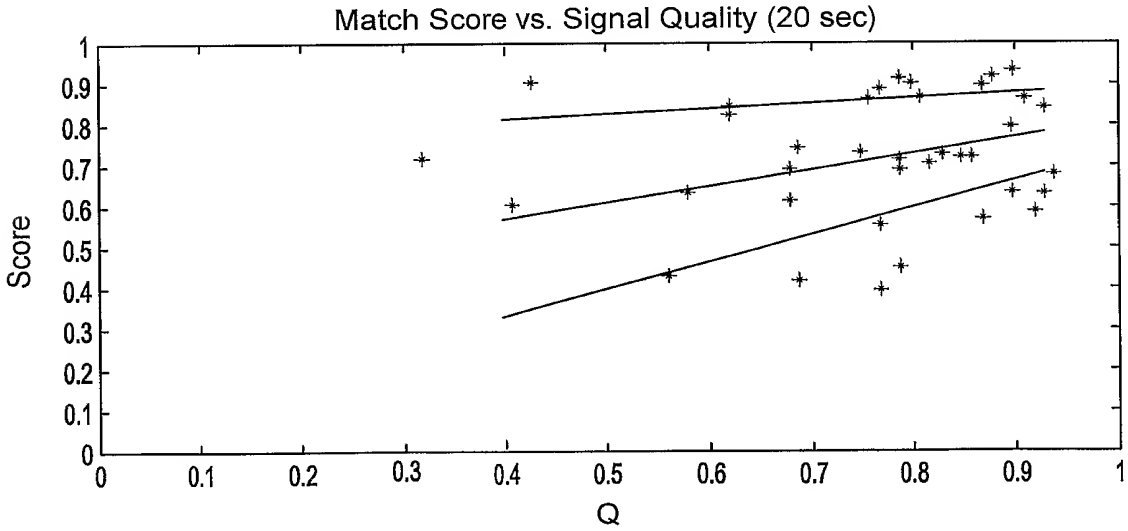


Figure 16: Match score distribution as a function of signal quality (20 sec segments)

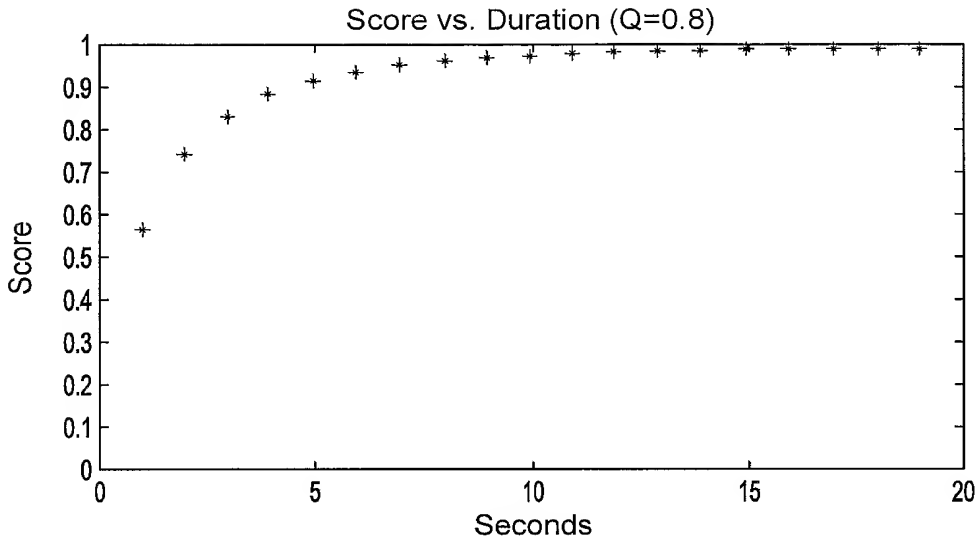


Figure 17: Match score as a function of duration of recording (Q=0.8)

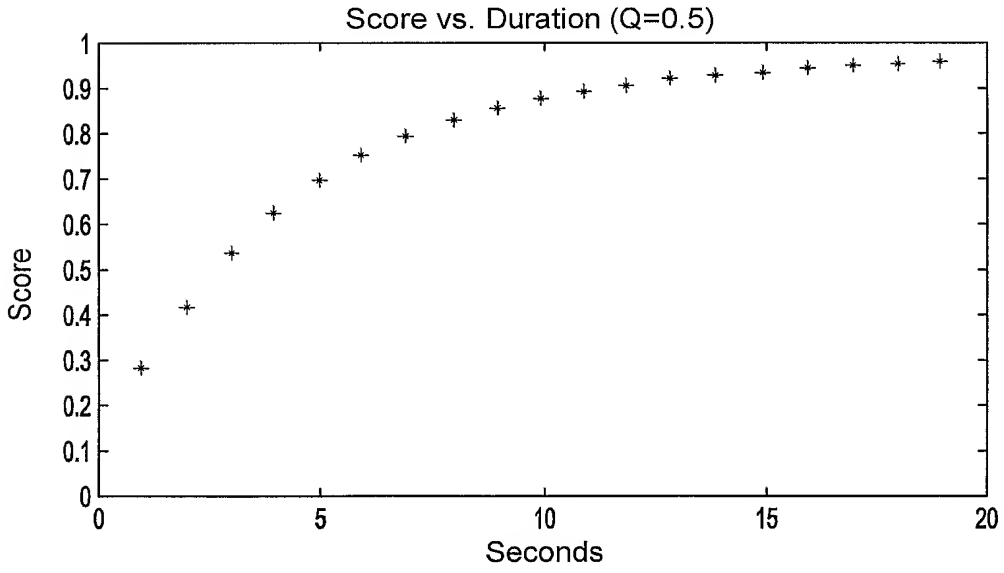


Figure 18: Match score as a function of duration of recording (Q=0.5)

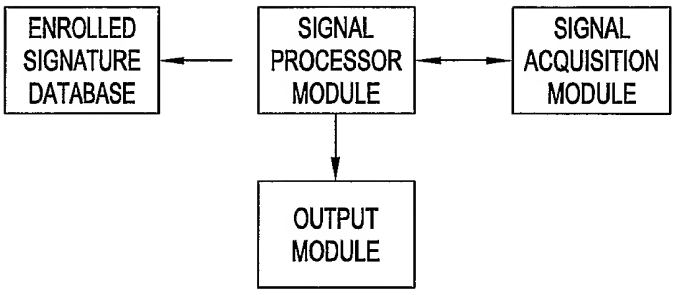


Figure 19

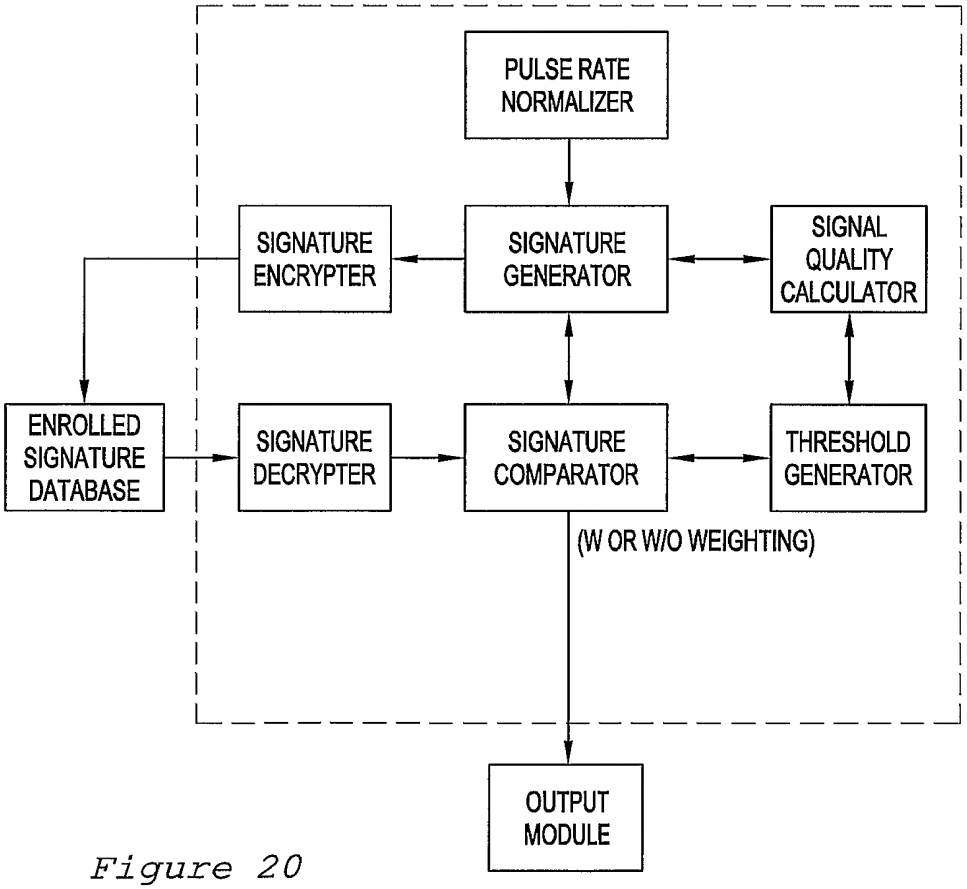


Figure 20

DERWENT-ACC-NO: 2006-502408

DERWENT-WEEK: 200864

TITLE: Identification method for electro-biometric identity recognition, involves determining selected individual to be specific individual when biometric signature of selected individual is same as specific individual

INVENTOR: LANGE D H

PATENT-ASSIGNEE: IDESIA LTD[IDESN]

PRIORITY-DATA: 2004WO-IB003899 (November 8, 2004)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
WO 2006059190 A2	June 8, 2006	EN
EP 1815391 A2	August 8, 2007	EN
AU 2005310994 A1	June 8, 2006	EN
KR 2007085857 A	August 27, 2007	KO
JP 2008518709 W	June 5, 2008	JA
CN 101263510 A	September 10, 2008	ZH

DESIGNATED-STATES: AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KM KN KP KR KZ LC LK LR LS LT LU LV LY MA MD MG MK MN MW MX MZ NA NG NI NO NZ O M PG PH PL PT RO RU SC SD SE SG SK SL SM SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW AT BE BG BW CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IS IT KE LS LT LU LV MC MW MZ NA NL OA PL PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW AL AT BA BE BG CH CY C Z DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR YU

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
WO2006059190A2	N/A	2005WO-IB003281	November 8, 2005
AU2005310994A1	N/A	2005AU-310994	November 8, 2005
CN 101263510A	N/A	2005CN-80037902	November 8, 2005
EP 1815391A2	N/A	2005EP-850656	November 8, 2005
EP 1815391A2	PCT Application	2005WO-IB003281	November 8, 2005
KR2007085857A	PCT Application	2005WO-IB003281	November 8, 2005
JP2008518709W	PCT Application	2005WO-IB003281	November 8, 2005
CN 101263510A	PCT Application	2005WO-IB003281	November 8, 2005
JP2008518709W	N/A	2007JP-539648	November 8, 2005

KR2007085857A	Based on	2007KR-712836	June 7, 2007

INT-CL-CURRENT:

TYPE	IPC DATE
CIPP	A61B5/0402 20060101
CIPP	A61B5/117 20060101
CIPP	G06K9/00 20060101
CIPP	G06K9/00 20060101
CIPS	A61B5/0402 20060101
CIPS	G06F21/20 20060101
CIPS	G06T7/00 20060101

RELATED-ACC-NO: 2004-144155 2006-343526

ABSTRACTED-PUB-NO: WO 2006059190 A2

BASIC-ABSTRACT:

NOVELTY - A biometric signature that identifies a specific individual is produced by forming the difference between the heartbeat pattern of the specific individual and the common features of heartbeat patterns. A biometric signature of a selected individual is obtained. The selected individual is determined to be the specific individual when the biometric signature of the selected individual is that same as the specific individual.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(A) an identification apparatus;

(B) a biometric identification system;

(C) a lock;

(D) a room access control device;

(E) a method for biometric identification;

(F) a method for locking a security device;

(G) an age analyzer; and

(H) a method for age detection.

USE - For electro-biometric identity recognition or verification. For use in e.g. automatic banking services, e-commerce, e-banking, e-investing, e-data protection, remote access to resources, e-transactions, work security, anti-theft devices, criminologic identification, secure entry, and entry registration in the workplace.

ADVANTAGE - Provides a reliable, robust, hard to deceive, low cost, user friendly identity recognition technology that may be used in stand alone applications or integrated with existing security systems.

DESCRIPTION OF DRAWING(S) - The figure shows the original electrocardiographic signals and their respective signatures constructed by eliminating the optimal combination of the three most influential PCs and their latency shifted versions.

CHOSEN-DRAWING: Dwg.5/20

TITLE-TERMS: IDENTIFY METHOD ELECTRO RECOGNISE DETERMINE SELECT INDIVIDUAL SPECIFIC SIGNATURE

DERWENT-CLASS: S05 T01 T04 T05

EPI-CODES: S05-D01B5; S05-D01C5A; T01-C08B; T01-N01A1; T01-N01A2A; T01-N02B1H; T04-D04; T04-D07F; T05-D01B;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: 2006-404193